1990-03

A proposed message system architecture for a Marine Corps Base implementation of the Defense Message System (DMS)

Weigand, John F.

Monterey, California: Naval Postgraduate School

(2)

NAVAL POSTGRADUATE SCHOOL

Monterey, California

THESIS

A PROPOSED MESSAGE SYSTEM ARCHITECTURE FOR A MARINE CORPS BASE IMPLEMENTATION OF THE DEFENSE MESSAGE SYSTEM (DMS)

by

John F. Weigand
March, 1990

Thesis Advisor: Norman F. Schneidewind

Unclassified

security classification of this page

REPORT DOCUMENTATION PAGE

1a Report Security Classification Unclassified	1b Restrictive Markings
2a Security Classification Authority	3 Distribution Availability of Report
2b Declassification Downgrading Schedule	Approved for public release; distribution is unlimited.
4 Performing Organization Report Number(s)	5 Monitoring Organization Report Number(s)
6a Name of Performing Organization: Naval Postgraduate School; 6b Office Symbol (*if applicable*) 32	7a Name of Monitoring Organization: Naval Postgraduate School
6c Address (*city, state, and ZIP code*): Monterey, CA 93943-5000	7b Address (*city, state, and ZIP code*): Monterey, CA 93943-5000
8a Name of Funding/Sponsoring Organization; 8b Office Symbol (*if applicable*)	9 Procurement Instrument Identification Number
8c Address (*city, state, and ZIP code*)	10 Source of Funding Numbers: Program Element No | Project No | Task No | Work Unit Accession No

11 Title (*include security classification*)
A PROPOSED MESSAGE SYSTEM ARCHITECTURE FOR A MARINE CORPS BASE IMPLEMENTATION OF THE DEFENSE MESSAGE SYSTEM (DMS)

12 Personal Author(s) John F. Weigand

13a Type of Report	13b Time Covered	14 Date of Report (*year, month, day*)	15 Page Count
Master's Thesis	From To	March 1990	107

16 Supplementary Notation The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

17 Cosati Codes			18 Subject Terms (*continue on reverse if necessary and identify by block number*)
Field	Group	Subgroup	Defense Message System, Naval message, computer networking, Thesis, SD.

19 Abstract (*continue on reverse if necessary and identify by block number*)

The current Automatic Digital Network (AUTODIN) communications system provides excellent message communications service within the Defense Communications System. However, AUTODIN speed of service objectives end at the Telecommunications Center (TCC). This gap between AUTODIN and end-user organizations causes delays and frustration to users who expect minimal delay in writer-to-reader message service. The Defense Message System (DMS) promises to deliver true writer-to-reader message service by extending automation from the TCC to the organizational level DMS also promises to standardize message communication services for DOD Services Agencies. This paper proposes a phased DMS implementation for a Marine Corps Base (MCB). Additionally, the protocol conversion processes illustrate some significant issues present during the transition to DMS. The intent of this paper is to suggest a network topology to implement DMS with additional dividends of using this topology with minimal rehabilitation in implementing succeeding DMS phases

Weigand

20 Distribution Availability of Abstract	21 Abstract Security Classification	
☒ unclassified unlimited ☐ same as report ☐ DTIC users	Unclassified	
22a Name of Responsible Individual: N.F. Schneidewind	22b Telephone (*include Area code*): (408) 646-2719	22c Office Symbol: 54SS

DD FORM 1473,84 MAR 83 APR edition may be used until exhausted
All other editions are obsolete

security classification of this page

Unclassified

Approved for public release; distribution is unlimited.

A Proposed Message System Architecture for a Marine Corps Base Implementation of the Defense Message System (DMS)

by

John F. Weigand
Captain, United States Marine Corps
B.S., University of Nebraska, 1980

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN TELECOMMUNICATIONS SYSTEM MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 1990

Author: [redacted]
John F. Weigand

Approved by: [redacted]
N.F. Schneidewind, Thesis Advisor

[redacted]
M.J. McCaffrey, Second Reader

[redacted]
David R. Whipple, Chairman,
Department of Administrative Sciences

ABSTRACT

The current Automatic Digital Network (AUTODIN) communications system provides excellent message communications service within the Defense Communications System. However, AUTODIN speed of service objectives end at the Telecommunications Center (TCC). This gap between AUTODIN and end-user organizations causes delays and frustration to users who expect minimal delay in writer-to-reader message service. The Defense Message System (DMS) promises to deliver true writer-to-reader message service by extending automation from the TCC to the organizational level. DMS also promises to standardize message communication services for DOD Services/Agencies. This paper proposes a phased DMS implementation for a Marine Corps Base (MCB). Additionally, the protocol conversion processes illustrate some significant issues present during the transition to DMS. The intent of this paper is to suggest a network topology to implement DMS with additional dividends of using this topology with minimal rehabilitation in implementing succeeding DMS phases.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

I. INTRODUCTION

"You cannot plan the future by the past. -----Edmund Burke"

A. BACKGROUND

The advent and rapid evolution of computer technology has led to the conclusion that the traditional Automatic Digital Network (AUTODIN) method of providing communications service by a separate communications facility is inadequate in meeting the Department of Defense's (DOD) communications needs. This notion is further reinforced by the gap created between the line of demarcation for AUTODIN services at the Telecommunications Center (TCC) and the organizational user. The current nature of narrative message processing coupled with the large amount of personnel staffing required for communications facilities is now more expensive than the equipment used to run communications facilities. This situation has led to the plan to extend automation to the organizational user. This extension is intended to satisfy the need for AUTODIN-style true writer-to-reader information exchange. The Defense Message System (DMS) is the project that intends to accomplish such a goal, not only for narrative message traffic, but also for electronic mail (E-mail) through office automation. Innovative planning and equipment is needed to accomplish this goal.

B. SCOPE

The purpose of this thesis is to familiarize those personnel who are unaware of DMS concepts and to propose a means to implement DMS. The Marine Corps' implementation of DMS is the major focus of this paper. DMS is so expansive that it is beyond the scope of this thesis to examine the total implementation of DMS. The focus of this paper is on the organizational implementation of DMS aboard a Marine Corps Base (MCB), using MCB Camp Pendleton, California as a model. The emphasis of this implementation structure is a topology that an organization may use to extend AUTODIN to an Automated Information System (AIS). This paper examines the AUTODIN message issues affecting an organization in implementing DMS on a MCB.

C. THESIS OUTLINE

1. Purpose

This paper proposes a viable architecture for a MCB to implement a phased migration to DMS. Wise management of scarce resources and interoperability issues

provide an impetus towards an expeditious implementation of DMS. This thesis will provide the management procedures and network topology to effectively implement DMS within the DMS development timetable. Ultimately, this implementation process will build upon the phased implementation process, rather than build from nothing in each phase.

2. **Chapter I. Introduction**

This chapter identifies the problem area to be solved by this paper. This chapter also provides an overview of the remainder of the paper, and identifies the scope of this paper. The purpose of this paper is outlined, and the research direction of this paper is defined.

3. **Chapter II. Problem Definition and DMS Concepts**

A discussion of current message handling systems is provided to empha size the rationale behind the need to change the present message handling system. This introductory chapter also describes DMS components and the DMS implementation strategy. Understanding where message handling systems are evolving provides an understanding of the processes in Chapters II and III.

4. **Chapter III. Office Automation Message Transfer**

RFC-822 is the E-Mail protocol specification used within Simple Mail Transfer Protocol (SMTP) in the Internet. RFC-822 message format is evaluated for its use as a preexisting basis for supplanting JANAP-128 protocol for interacting with X.400 and the OSI protocol suite in the AUTODIN system. The discussion in this chapter examines the interaction of RFC-822 message format and JANAP-128 format. RFC-822 is a widely used protocol and can be mapped to the DMS protocol, X.400. This protocol conversion forms the basis for use with the architecture discussed in Chapter IV. This chapter discusses system security and authentication issues.

5. **Chapter IV. A Proposed Marine Corps Base Implementation of DMS**

This chapter proposes a MCB network structure for implementing DMS. Patterned after the Navy Network Management Center (NMC), and the Navy Base Information Transfer System (BITS), this network is designed to provide the automated message handling needs for a Marine Corps Base organization. This chapter discusses security issues, message management procedures, message preparation procedures, signature verification issues, and network topology.

6. **Chapter V. Summary and Conclusions**

This chapter provides a summary of the DMS implementation issues. The key points of the proposed MCB topology for the migration of existing systems towards the

ultimate DMS target architecture are also summarized in this chapter. Potential thesis topics are discussed in this chapter to aid readers interested in DMS topics.

II. PROBLEM DEFINITION AND DMS CONCEPTS

A. METHODOLOGY

To examine this radical departure from traditional AUTODIN procedures, we must first define a valid set of user requirements, examine what is currently designed to fulfill those requirements, evaluate the effectiveness of the current system, design enhancements, or devise solutions to any shortfalls in the current system, and implement the solution to those shortfalls.

1. User Requirements

DOD users are globally oriented, and multiservice, so that any message system requires global connectivity, and must be interoperable with other Services, and Allied nations. This connectivity carries a responsibility for the following needs:[Ref. 1]

a. Guaranteed delivery

An assurance of guaranteed delivery of an electronic message from an authorized writer to an authorized reader. Concurrent with this is the guarantee that the message is not inordinately delayed despite the amount of processing within the system.

b. Security

A secure means of delivering messages using cryptographic techniques. This also includes shielding sensitive messages from misrouted messages.

c. Accuracy

Messages are delivered accurately and completely. Corrections to messages cause unacceptable delays for messages which require a timely response from the recipient.

d. Precedence system

A hierarchical system of message importance is established for critical or sensitive messages. This procedure allows an override capability for urgent and important messages.

e. Effective routing

Messages are quickly delivered to the intended recipient within an organization without multiple layers of manual processing which could slow the delivery time.

f. Simple rules

The message system must be friendly enough to allow a user to easily send or receive messages with a degree of flexibility or tolerance. There must be an effective

and robust training and system documentation environment which enables users to learn how to operate the system with a minimum of time.

2. Current message processing system

AUTODIN was established in the 1960s to provide secure, automated store-and-forward message service to meet the operational requirements of the DOD [Ref. 2: p. 3-1]. The worldwide communications network has 15 operational Automatic Switching Centers (ASCs), and 2 test ASCs. These ASCs perform store-and-forward message switching functions, some message validation functions, message format conversion, and some specialized routing functions. Rounding out the view of AUTODIN, a communications network is defined as:[Ref. 3: p. 2-1]

> Communications Network - A group of computers joined together by data-carrying links. Data links could include long-haul telephone links, satellite relays, fiberoptic cables, or radio links.

a. AUTODIN equipment

Automated Message Processing Exchanges (AMPE) interact with this communications network, with each Service typically having its own AMPE to meet its mission requirements. Table 1 lists some examples of AMPEs.

Table 1. AMPE EXAMPLES

Organization	AMPE
USA	Automated Multi-Media Exchange (AMME)
USN	Local Digital Message Exchange (LDMX)
USAF	Air Force Automated Message Processing Exchange (AFAMPE)
NSA	Streamliner
DIA	Communications Support Processor (CSP)

Communications networks that formerly were the exclusive domain of communicators are now pervaded throughout the networks by computers as planners attempted to automate AUTODIN in response to increasing volumes of messages. These automation attempts have reduced the amount of burdens placed on manual processing, and now have the potential to place the communications function at the organizational user level. AMPE's are automated to an extent and provide limited switching functions for attached terminals, plus other features such as converting destination names (Plain Language Addresses (PLA) into Routing Indicators (RI)), and de-

termining the distribution of messages. Automation of AUTODIN can be illustrated in a definition of AUTODIN:

> AUTODIN - A worldwide Department of Defense computerized general purpose network.[Ref. 3: p. 8-1]

Some portions of AUTODIN are obsolescent to the point that costly maintenance is required and it is difficult to incorporate enhancements to compensate for deficiencies.

Staffing of the AUTODIN system was less expensive than providing and maintaining the equipment in the early development of AUTODIN. The reverse is largely true today. The annual cost of maintaining AUTODIN has been estimated at S2B [Ref. 2: p. 3.3]. The manual aspect of TCC processing, in addition to manual DD-173 preparation and organizational Message Center processing, highlight the benefits of using office automation to send messages and strive for true writer-to-reader connectivity.

The TCC is the principal entry and exit point for AUTODIN messages. Narrative messages are generally entered via Optical Character Reader Equipment (OCRE). The DD-173 message form is the standard form used by the Navy used to scan a message by using OCRE and transmitting it via AUTODIN. manually prepared by the organizational user, and delivered to the TCC for scanning into ASCII characters and transmitted over AUTODIN for delivery to the recipient[Ref. 4]. An organization's Message Center is generally the interface between the user and the TCC. The TCC processes messages both to and from an organization through Over-The-Counter (OTC) service. This manual processing introduces errors and delays to transmitting messages. Further manual processing delays are introduced where messages are manually reproduced for the required number of copies. Data pattern message traffic is also transmitted by using magnetic tape reels in the same manner as the DD-173 message form is used for narrative messages.

Due to the organizational nature of the PLA, messages are delivered on the basis of the RI through AUTODIN only to that official name. Office codes/symbols supplementing PLA's are an effort to enhance delivery to the intended action officer/section within an organization. A lack of published standard office codes, symbols degrade this effort. This is especially true in large organizations, where misrouted, or misassigned messages may be delayed for days. Misrouting due to inap-

propriate PLA could be even worse, because of the manual processing required to service the message, and such messages could possibly be lost in the AUTODIN system.

3. Phased DMS solution

The phased implementation of the DMS promises to gradually extend automation from the AUTODIN line of demarcation at the TCC effectively down to an organization's office automation. This transition is planned to occur over a period of 20 years from 1988 to 2008. Initially, Non-Developmental Items (NDIs) and modification of existing equipment are to incorporate at least OTC diskette service, and possibly allow a Personal Computer (PC) or Local Area Network (LAN) direct connection to the TCC. The migration process from AUTODIN to DMS is briefly described below[Ref. 2: Pp. 2.10 - 2.15]:

a. Baseline DMS

The baseline phase for DMS will use AUTODIN for its backbone network and the AMPE will be either linked directly to office automation, or will process diskettes through OTC service at the TCC. Figure 1 on page 8 shows the Baseline architecture [Ref. 2: p. 2-11].

b. Phase I

DMS Phase I is targeted for completion by 1993. This phase is designed to extend TCC services down to the organizational user level, to add an AUTODIN-to-Defense Data Network (DDN) Interface (ADI), and to migrate data pattern traffic to the DDN. Figure 2 on page 9 shows the Phase I architecture [Ref. 2: p. 2.16].

c. Phase II

DMS Phase II is targeted for completion by 2000. This phase is to present an integrated DMS (i.e., incorporate video, data, and narrative messages), and begins to phase out the TCC's. Figure 3 on page 10 shows the Phase II architecture [Ref. 2: p. 2.17].

d. Phase III

DMS Phase III, the last phase, is targeted for completion by 2008. DMS is to be fully integrated with an Integrated Services Digital Network (ISDN) based long-haul and base level communications structure. Figure 4 on page 11 shows the Phase III architecture[Ref. 2: p. 2.19].

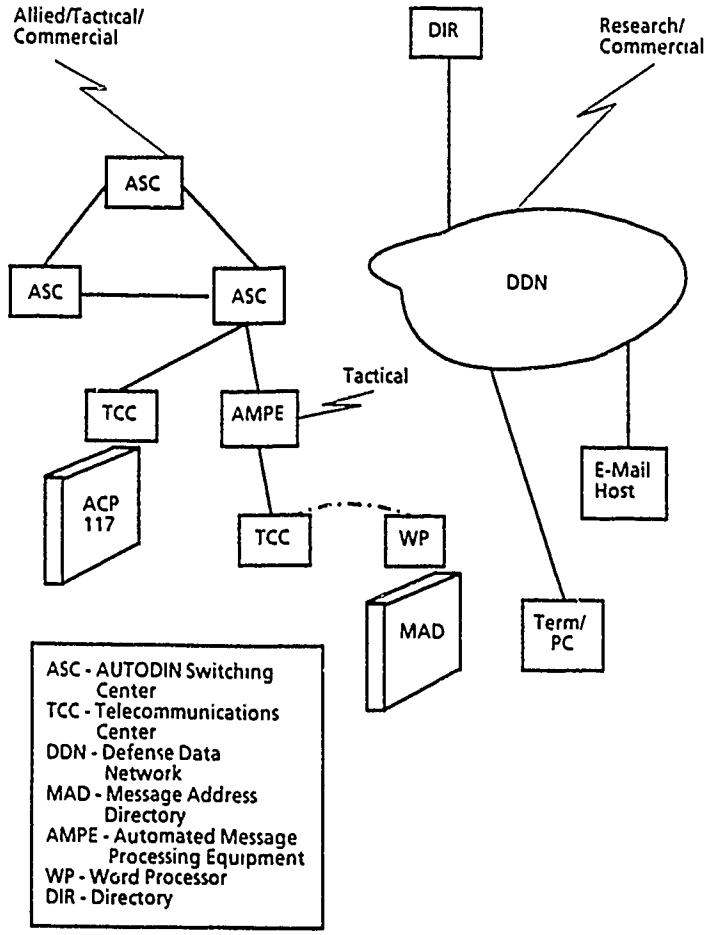


Figure 1. Baseline DMS Architecture

B. DEFENSE MESSAGE SYSTEM SOLUTIONS

DMS promises to fulfill true writer-to-reader service through its phased implementation by gradually increasing the degree of automation in the message system. In implementing DMS, the project is managed by the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)(ASD(C^3I)) using the following management structure as depicted in Figure 5 on page 12 [Ref. 2: p. 2-7]:

- ASD(C^3I) - The ASD(C^3I) is responsible for establishing DMS policy
- Military Communications and Electronics Board (MCEB) -The MCEB is responsible for establishing DMS procedures.
- Joint Chiefs of Staff (JCS) - The JCS is responsible for establishing the requirements for DMS

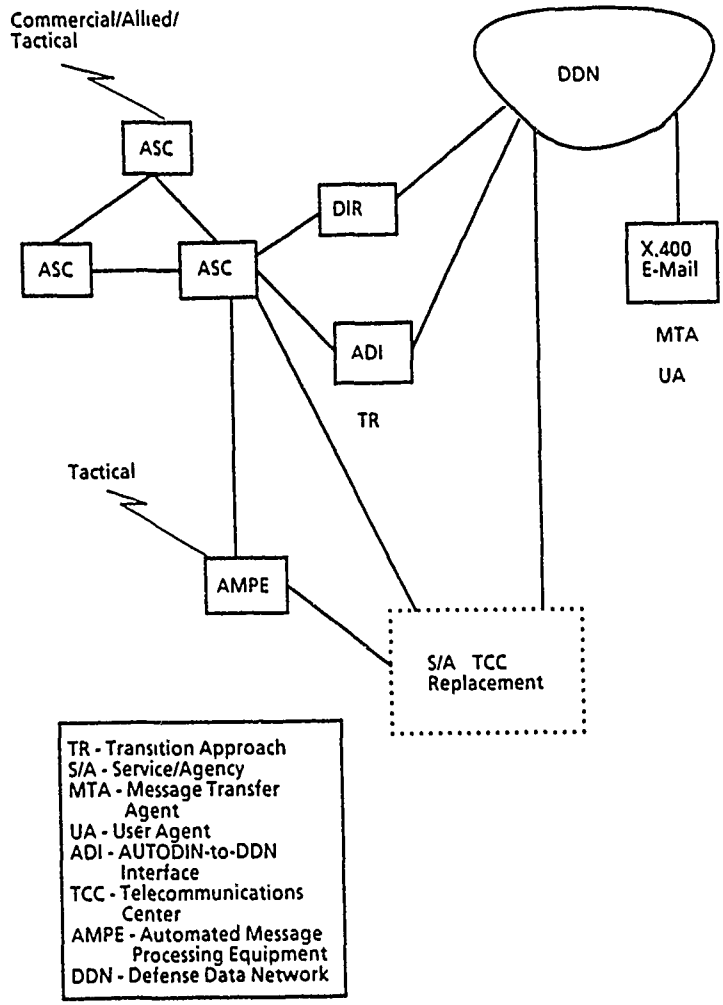


Figure 2. Phase I DMS Architecture

- Defense Acquisition Board (DAB) - The DAB is responsible for the acquisition of DMS components.
- DMS Panel - The Director, Information Systems chairs this panel comprised of members from the following:
  - MCEB
  - OJCS(J6)
  - Services Agencies Representatives
- DMS Coordinator - The DMS Coordinator is responsible for the execution of the DMS project, and works for the Director, Defense Communications Agency. Working for the DMS Coordinator are the following members:

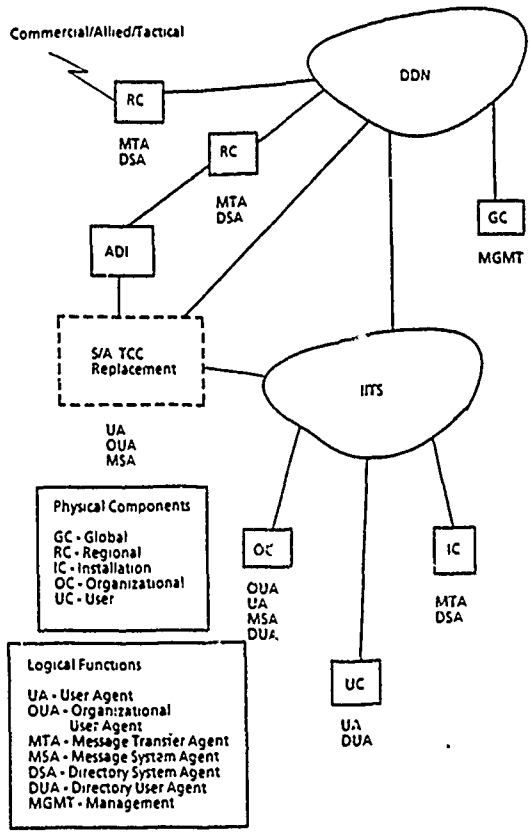


Figure 3. Phase II DMS Architecture

- Testbed Managers - These managers are responsible for testing and evaluating DMS components, and to streamline the acquisition process.
- Service Agency Coordinator - They will be the focal point for their Service Agency on the DMS project.
- DMS Project Managers - They will have development, testing, and deployment responsibilities.

C. DMS MESSAGES

AUTODIN messages are bundled into one category, i.e., official organizational messages that are difficult to deliver to a specific entity within the organizational PLA. DMS messages are more flexible with respect to delivery to entities within an organization. The definition for DMS provides a general understanding of DMS messages:[Ref. 2: p. 1.4]

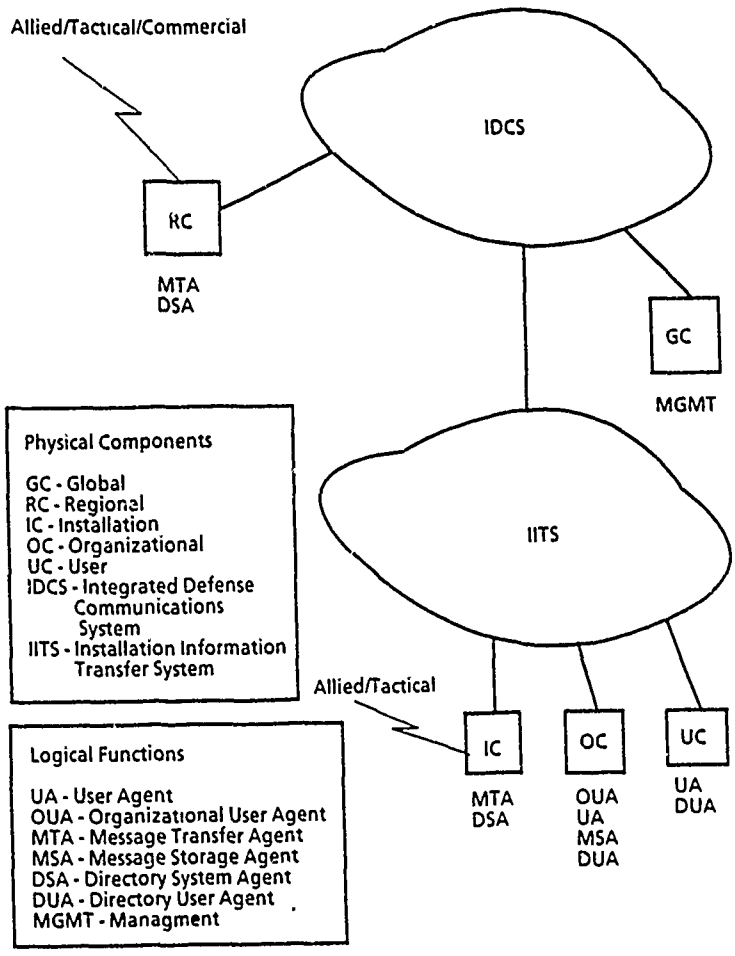


Figure 4. Target DMS Architecture

Defense Message System - The DMS is all systems used for the electronic delivery of messages in the DOD between organizations and individuals.

Conceptually, DMS will be comprised of AUTODIN (including base level TCC's) and Electronic Mail (E-Mail) on the DOD Internet (DDN and associated LAN's). DMS messages are labeled within two broad categories[Ref. 2: p. 1-3]:

1. Organizational

These messages require approval for transmission by designated officials of the sending organization. Due to their official and sometimes critical nature, such messages can be directive in nature, and impose operational requirements on communications systems for their delivery. An organizational message is one that includes command and control messages exchanged between organizational elements.

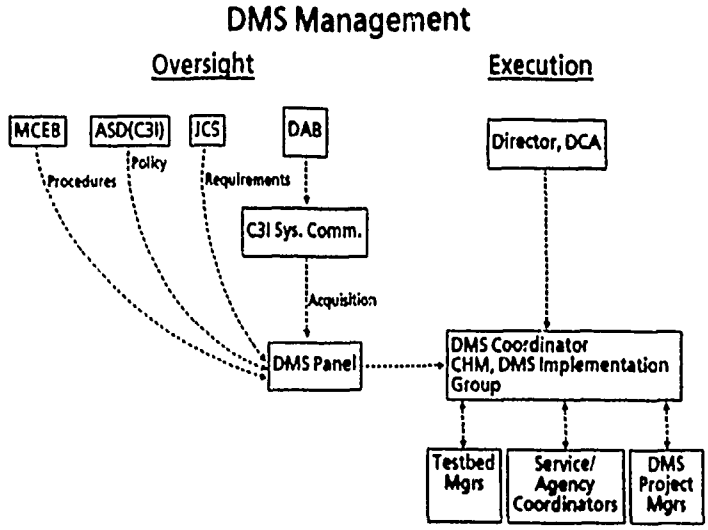


Figure 5. DMS Implementation Management Group

2. Individual

These messages include working messages between individual DOD personnel within administrative channels, both internal and external to an organization. A basic transport service is all that is required of the communications system for these messages, as they do not generally commit or direct an organization.

D. DMS SCOPE

DMS is intended to fill more than narrative message needs. A discussion follows on the elements of DMS to provide a broad perspective on what is entailed in DMS:

1. AUTODIN

AUTODIN will initially provide the backbone system for primarily narrative message traffic. As DMS implementation progresses, AUTODIN systems will be increasingly required to interface with office automation systems. The X.400 Message Handling System (MHS) protocol has been adopted as the DMS standard. Because the JANAP-128 protocol is used in AUTODIN today, there must be a gateway which converts JANAP-128 protocol to the protocol implemented during the DMS transition process. Chapter III discusses the issues and processes of protocol conversion for AUTODIN messages. Like AUTODIN, X.400 makes use of the store-and-forward Message Transfer System (MTS)[Ref. 5: p. 4].

2. E-Mail

The Defense Data Network (DDN) E-mail service is to provide the transportation services for the bulk of data communications services for DOD Services/Agencies[Ref. 6]. Although not a compor nt of DMS, the DDN provides a means for providing Individual message service until the DCS has migrated to a true DMS structure with X.400. DDN provides E-mail services using a proven E-Mail system, the RFC-822 format within Simple Mail Transfer Protocol (SMTP). Providing a gateway between RFC-822 message format and JANAP-128 message format during the migration to X.400 facilitates a smooth transition to DMS. DDN has several components:

- Host computers supporting electronic mail
- User terminal Personal Computers (PC)
- On-line directories, i.e., Network Information Center (NIC)
- DOD Classified Internet
  - Defense Secure Network 1 (DSNET1) - Classified General Service (GENSER) messages.
  - DSNET2 - Worldwide Military Command and Control System (WWMCCS) classified messages.
  - DSNET3 - Sensitive Compartmented Information (SCI) classified messages.
- DOD Unclassified Internet
  - Unclassified DDN (MILNET, ARPANET).

Appendix B shows the general configuration of the DDN components[Ref. 7: Pp. 7-1 - 7-6]. Eventually the individual DSNETs will be consolidated into a Multilevel Secure (MLS) network called the Defense Integrated Secure Network (DISNET). All of the equipment used on these networks can double as a general purpose Automatic Data Processing (ADP) machine as well as an electronic mail handler.

3. Protocols

Computer communication protocols are rules used to control data transfer among network components which state how messages are electronically formatted within a network[Ref. 8]. The relationship between a baseball pitcher and catcher is a close analogy of the function protocols serve in a network. Their signals passed between each other control the events during a baseball game, similar to the way that protocols control events in a communications network. The following is a brief description of the protocols used in DMS:

a. Open Systems Interconnection (OSI) Protocols

The ASD(C^3I) has declared that the Government Open Systems Interconnection Profile (GOSIP) will be adopted as the DOD set of protocols used in DMS, starting two years from the formalization of the Federal Information Processing Standard (FIPS) [Ref. 9]. The FIPS was formalized in August, 1988. All DOD protocols after August, 1990 must comply with the GOSIP, while maintaining interoperability with existing DOD systems. The International Standards Organization (ISO) is developing these OSI protocol standards. The primary reason for DOD adopting such standards is to be fully interoperable with our allies, and to set a standard suite of protocols which economizes developmental efforts. Open systems architecture essentially means that any user may communicate with any other user on the network as various implementations of the protocol suite should result in compatible systems. This topic is discussed further in the succeeding chapter.

b. X.400 Message Transfer System

The essential data created by the organizational user is encapsulated within layers of computer header information, and is transferred within the OSI architecture based on the layers it encounters. X.400 provides a variety of services besides message handling services. The next chapter discusses the fields and capabilities of X.400.

c. X.500 Directory Services

This protocol provides the directory services within the DMS system, which is analogous to the Naval Computer Processing and Routing Service (NAVCOMPARS) in determining exactly where the electronic message should be delivered.

4. DMS Encryption

End-to-end (E^2) encryption will be by means of the National Security Agency's Secure Data Network System (SDNS). Addresses will be exposed for routing purposes within SDNS encryption, but the addresses will be link encrypted by means of KG-84A cryptographic devices. This encryption scheme protects the text from inadvertent exposure to unintended recipients of the message for E^2 service, but exposes the address at the node. Figure 6 on page 15 shows E^2 and link encryption[Ref. 7 : p. 7.3a]. For example, if the message were delivered to the wrong address based on the header information, the text would be protected by the E^2 encryption. Blacker Front End (BFE) devices are intended provide initial cryptographic security for the DDN.[Ref. 2] Figure 7 on page 16 shows a sample BFE implementation scheme[Ref. 7: p. 7-4a].

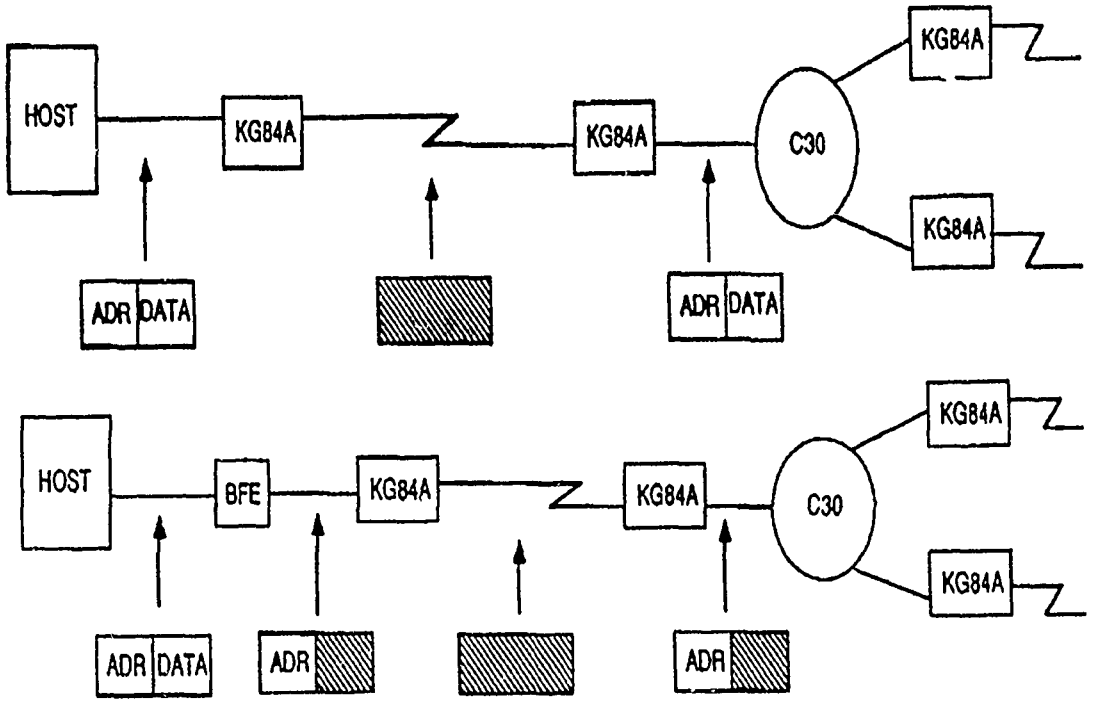


Figure 6. Link and E^2 Encryption

5. DMS Functionality

The following is a brief description of the functional components of DMS:[Ref. 2: Pp. 5-3 - 5-8]

a. DMS Physical Components

DMS physical components have very similar functionality to the AUTODIN components, as a result of the nature of the networking capabilities. The DMS physical components are called the following:

- Global Component (GC). Those components serving the entire DMS. Similar to the ASC in AUTODIN

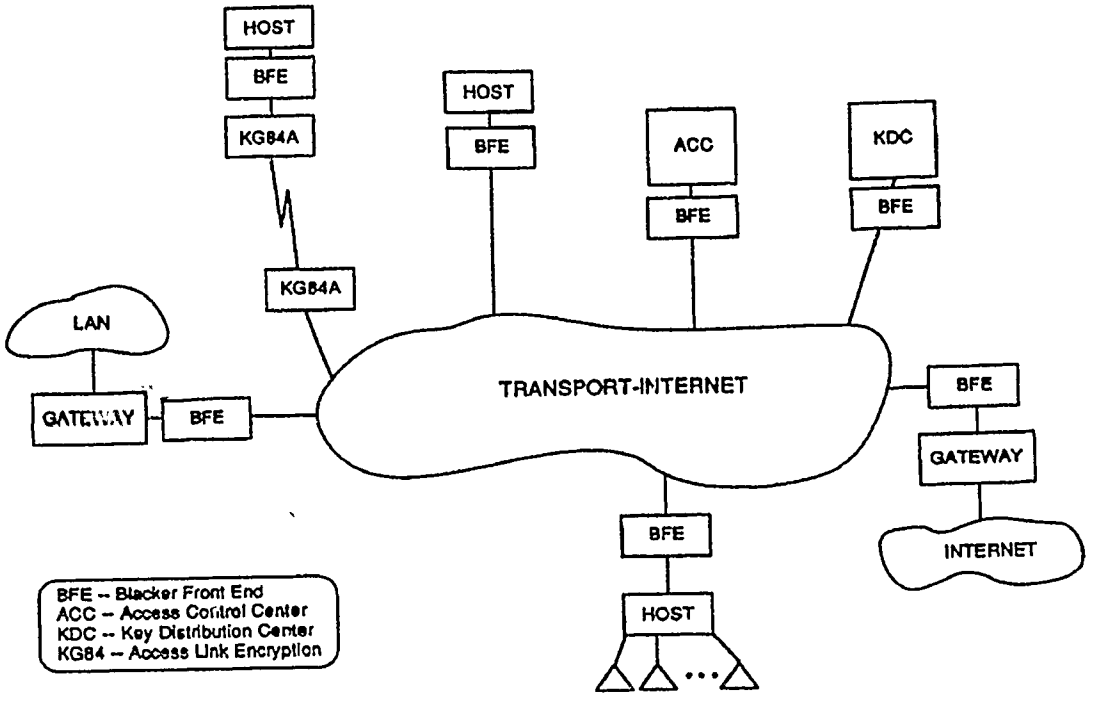


Figure 7. BLACKER Typical Application

- Regional Component (RC). Those components serving a large area, but less than the entire DMS. Similar to the AMPE, LDMX in AUTODIN
- Installation Component (IC). Those components serving a single post, camp, station, base, etc. Similar to the TCC in AUTODIN
- Organizational Component (OC). Those components serving an individual user. Similar to a LAN or office automation

b. DMS Logical Components

The logical components of DMS include the following elements:

- User Agent (UA) and Organizational User Agent (OUA). These act on behalf of the user to send and receive messages
- Message Storage Agent (MSA). These provide long term storage and retrieval

- Message Transfer Agent (MTA). These provide basic message relay capability and acting together with the Message Transfer Service (MTS), delivers messages via UAs/OUAs

Figure 8 on page 18 illustrates the DMS logical and physical components [Ref. 2: p. 5.1].

E. DMS BASELINE PHASE

The DMS Baseline Phase is already in progress, and this phase will extend automation from the TCC to an organization using Non- Development Items where practical. In the short term, the TCC is to be modified with diskette processing capability in order to process diskettes OTC, maintaining compatibility with U.S. Joint Message Text Format (USJMTF) [Ref. 2: p. 2-3].

F. DMS PHASE I

DMS Phase I is designed to last until 1993. Table 2 shows the equipment to be phased out by the end of the period.

Table 2. SUPERSEDED EQUIPMENT

Digital Subscriber Equipment
DCT 9000 TCC Systems
Standard Remote Terminal (SRT)
AMME
Teletypewriter Models 23, 40
Honeywell CCT-07 TCC
Control Data Corporation CDC-1700
AFRAIDS (UNIVAC-418III)

Table 3 shows the formats/procedures to be phased out during this phase, again targeted for completion by the end of 1993.

Table 3. SUPERSEDED FORMATS/PROCEDURES

Non-standard E-Mail Formats/Procedure
ACP-127 U.S. Supp-1
ACP-126 Modified
JANAP-128
DOI-13 (Includes CRITIC)
Streamliner Abbreviated Message Format (AMF)
Abbreviated SI Format

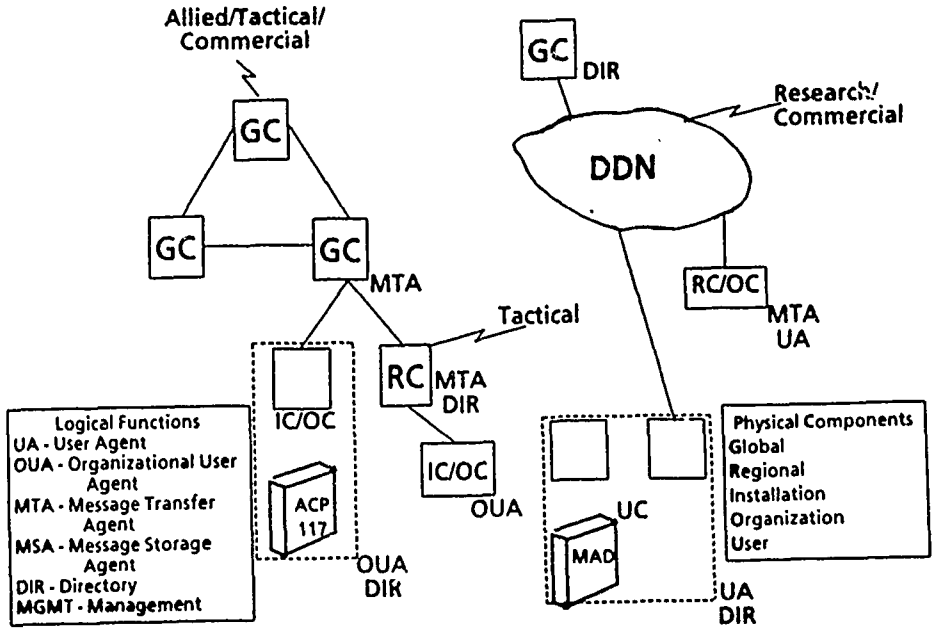


Figure 8. DMS Logical Components

1. Features introduced

- TCC services extended down to the organizational user
- Addition of the ADI
- SMTP to X.400 conversion
- Data pattern message traffic migrates to DDN
- DISNET integrated using BFE devices

2. Navy LAN Implementation Plan

The Navy plans to implement the Base Information Transfer System (BITS) as its standard Metropolitan Area Network (MAN) for the organizational user (Installation Information Transfer System (IITS) in DMS terms). Figure 9 on page 20 illustrates the general network structure of BITS[Ref. 10: p. 4-7]. OPNAVINST 2800.3 has

legitimized BITS as an approved standard MAN for the Navy. The long-range plans for this system is to be compatible with the ISDN, when ISDN is fully implemented DOD-wide. The following services are expected to be integrated into BITS:

- File transfer
- Interactive modes
- Electronic-Mail
- Video teleconferencing
- Security
- Voice communications

G. DMS PHASE II

DMS Phase II is targeted for completion by the year 2000. The objective of this phase is maximum automation. SDNS protection encrypts the message content while being transferred within the MTS, leaving minimal staffing and security protection. If MILNET and DISNET remain disjointed, then BFE devices will provide the cryptographic security for these networks. The following events are expected to occur during Phase II:

- TCC's are phased out
- ASCs evolve to X.500 DSA and X.400 MTA roles
- DSA functions assumed by the ASCs:
  - Directory management/maintenance
  - Cryptographic keying management
  - Monitoring network status
  - Configuration control

H. DMS PHASE III

DMS Phase III is targeted for completion by the year 2008, with its objective being the achievement of an ISDN based Integrated DCS (IDCS). IDCS will replace the longhaul portion of the DOD Internet, and DDN. The components of DMS will be located with the users vice the AUTODIN model of stand-alone communications facilities.

Sender authentication is intended to be achieved through the features of X.400 message protocol with its SDNS E^2 security architecture. ISDN by this point is meant to be a truly integrated network of video, voice, facsimile, and record traffic. Since all

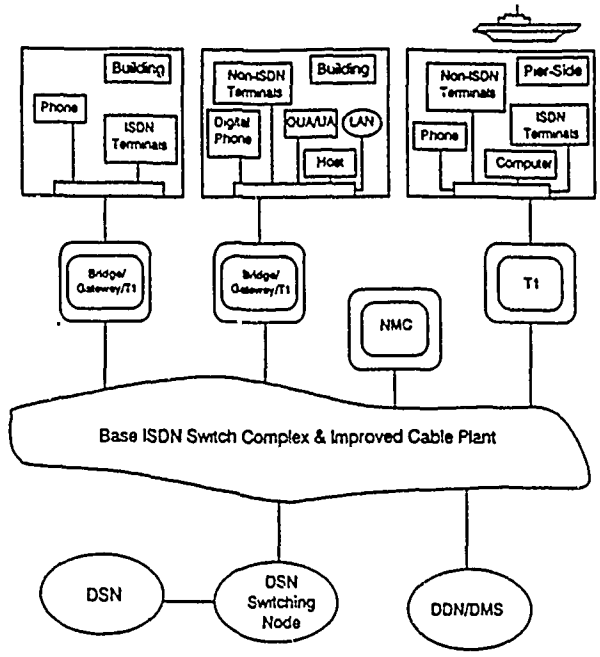


Figure 9. BITS Target Architecure

DMS users will be using the same standards, it is expected that this system will be a truly open system, with all DMS users able to communicate with any other DMS user.

I. CHAPTER SUMMARY

The DMS is an ambitious project that promises to provide true writer-to-reader connectivity for electronic messages. Budget cuts, personnel shortages, equipment obsolescence, and the lack of a standard DOD configuration have all conspired to solidify a resolve to develop such a system. The potentially high interoperability of such a standardized system among the DOD Services makes this proposal both appealing and plausible, as there is high interservice interest in making the system work. Similarly, there must be no loss of present capabilities for each service, otherwise DMS will lack the acceptance it needs to meet its goals.

Modern computer processing capabilities definitely have the potential for enabling this plan to succeed. The transition from stand-alone communications facilities to organizational level communication functions must be organized with the idea that the business of handling messages will evolve beyond AUTODIN style of processing mes-

sages. File transfers and E-Mail have seen to it that traditional concepts of paper messages need not be forced on such electronic systems. The procedures to manage such a system must be just as innovative as the equipment that will operate within DMS.

III. OFFICE AUTOMATION MESSAGE TRANSFER

A. BACKGROUND

The previous chapter gave the transition schedule towards OSI standards, and presented the terminology to understand DMS functionality. This chapter builds on the previous Chapter's terminology and uses this foundation to develop a discussion on message protocol trends and requirements for DMS implementation strategy. The message protocol issue is pivotal to the electronic message issue associated with migration to OSI standards because the handshaking agreements between equipments must be compatible in order to communicate.

1. Government Open Systems Interconnection Profile (GOSIP)

GOSIP became a FIPS in August 1988, and as mentioned in the previous chapter, it is the mandatory DOD standard for open networking after August 1990. The seven layers of the OSI Reference Model are shown in Figure 10 on page 23 [Ref. 11: p. 29]. Figure 11 on page 24 [Ref. 12: p. 82] shows the interpretation of the DOD protocol suite against the OSI Reference Model.

The OSI Model is equally applicable to all types of computer networks, including mainframe architectures and LANs. The generalized structure of protocols for a LAN is depicted in Figure 12 on page 25[Ref. 13: p. 281]. The OSI Model as implemented in LANs is shown in Figure 13 on page 26 and Figure 14 on page 27.[Ref. 14: p.20] In Figure 13 on page 26 and Figure 14 on page 27, the lower layers are usually implemented in hardware, and the higher layers implemented in software[Ref. 7: p. 3-6].

The aims of GOSIP are to provide products that are interoperable, multi-vendor, and commercial off-the-shelf (COTS) procurements:[Ref. 11: p. 570]. GOSIP provides impetus for vendors to develop OSI compliant products[Ref. 15 : p. 27]. This is particularly true if the majority of the vendors seek the U.S. Government's business. It helps that the DOD policy on standards is to use commercial standards in preference to military standards if they meet military standards requirements[Ref. 16: p. 1]. Shopping for different vendors in the sense of developing a multi-vendor procurement vice sole source buying has potential equipment compatibility problems associated with it.

Vendors might select different GOSIP options from a given set of specifications and implement these standards in different ways from each other to such an extent that the devices do not work as a system once the components are assembled in the final

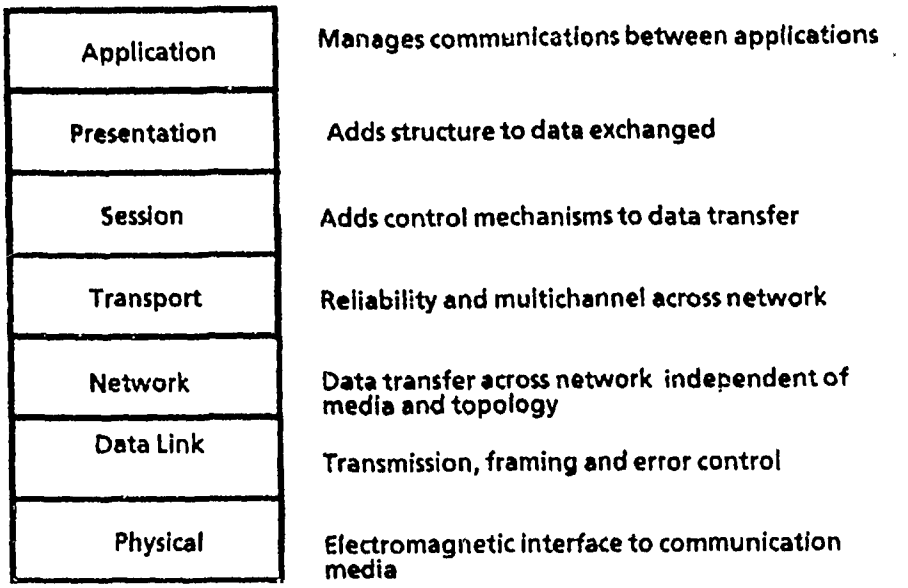


Figure 10. OSI Reference Model

configuration[Ref. 15: p. 30]. The National Institute of Standards and Technology (NIST) and the Corporation for Open Systems (COS) are responsible for conducting conformity tests on applications implemented by vendors. Theoretically, the open systems strategy allows greater probability of procuring systems from multi-vendor sources that do not have any compatibility problems in operation.

The main reasons for the transition from the DOD networking protocols to those specified by the OSI model are as follows[Ref. 16]:

- Reduced cost
- Increased interoperability
- Increased application-level functionality

This transition to OSI protocols will not occur overnight, although the DOD mandate for compliance to GOSIP certainly helps to accelerate the process. The Internet suite of protocols are widely implemented and provide satisfactory services to users. The transformation of DOD protocols to OSI standards will undergo phases of coexistence, transition, and convergence.

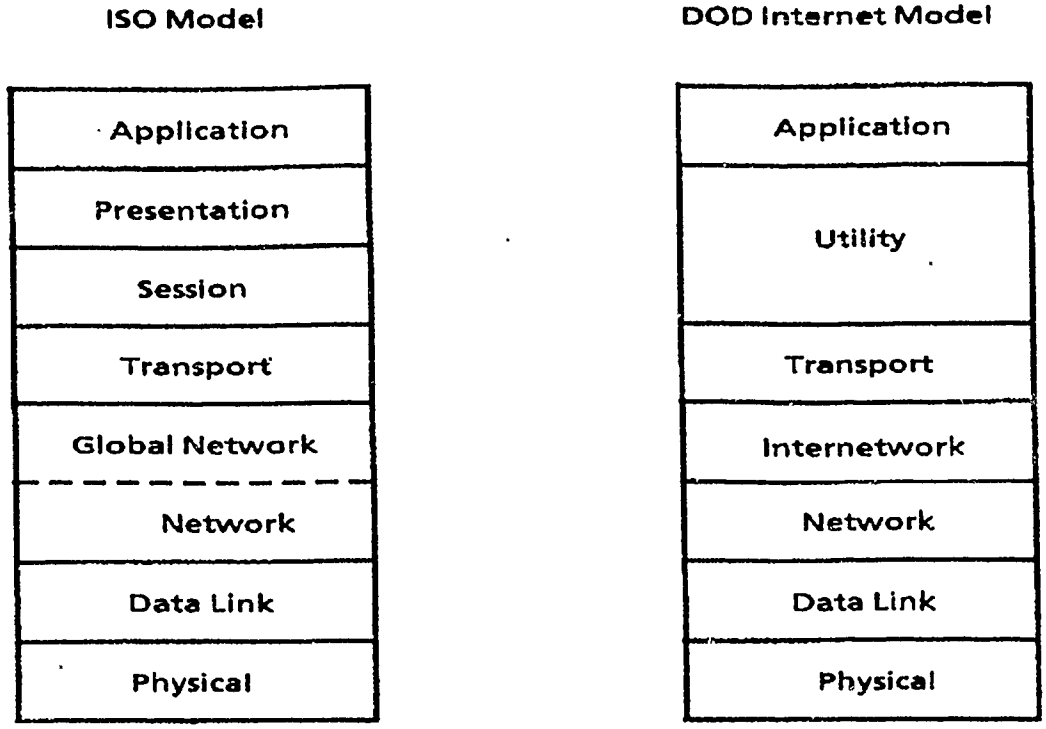


Figure 11. OSI and DOD Protocol Layers

The duration of these phases depend largely on the ability to map services across different protocols. There are two inhibitors to convergence as a total solution[Ref. 17: p. 2]:

- It is already too late. There is an installed base of over 20,000 SNA networks, 2,000 DECNet and several hundred TCP/IP networks, et al.
- Convergence implies that all tradeoffs are understood, and all necessary inventories are made and assimilated. Innovation in this context tends to interrupt and destabilize the convergence process.

Figure 15 on page 28 shows the protocol suites for these major architectures[Ref. 7: p. 4-18a].

2. GOSIP Implications for DMS

DMS, as a philosophy, is involved in only the message communications subset of the transition to OSI protocols and the related OSI layers to support electronic messaging. File transfers are not in the domain, per se, of DMS. The merging of the separate network operations which handle existing AUTODIN messages and DDN E-Mail messages involves the coexistence, transition and convergence issues mentioned earlier.

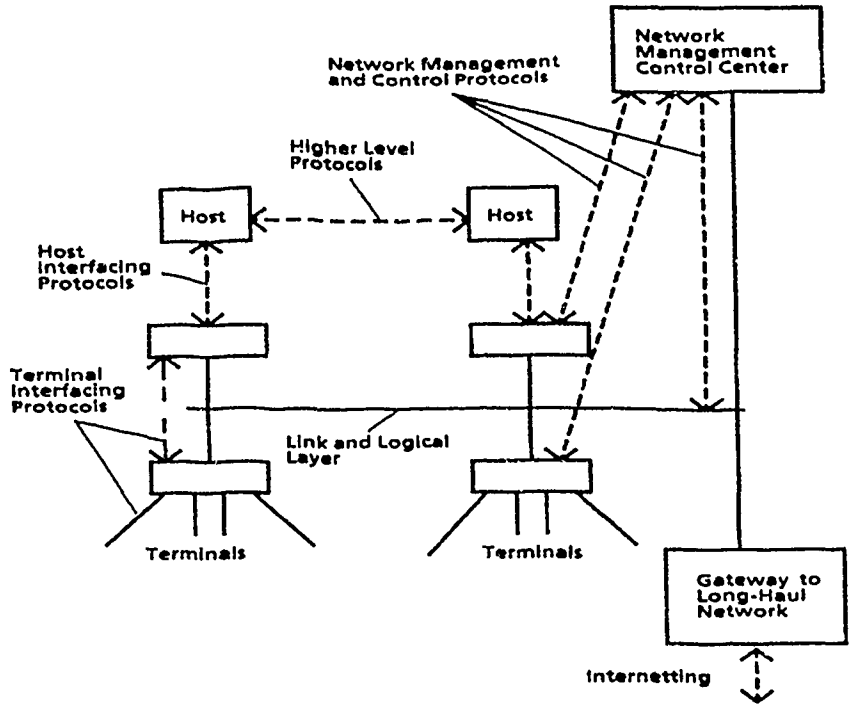


Figure 12. Protocols on a Local Network

There are three main methods of incorporating OSI protocols gradually and selectively into today's existing networking environment as follows[Ref. 15: p. 27]:

- OSI pilots
- Mixed protocol stacks
- Gateways

Whether the existing networks can be transformed into pure OSI networks, or should they be made into pure OSI networks is debateable. Allowing non-OSI protocol suites to act as underlying structures lends greater flexibility in implementing OSI. Strategies to convert protocols to OSI standards are discussed below.

B. OSI TRANSITION STRATEGIES

OSI protocols will achieve dominance over the Internet suite of protocols and AUTODIN protocols at some future point in time. DOD protocols must achieve OSI interoperability before the marketplace generally accepts the OSI protocols as the standard suite of protocols. The Baseline period extends the communications process to organizational office automation using existing protocols. The gradual transforma-

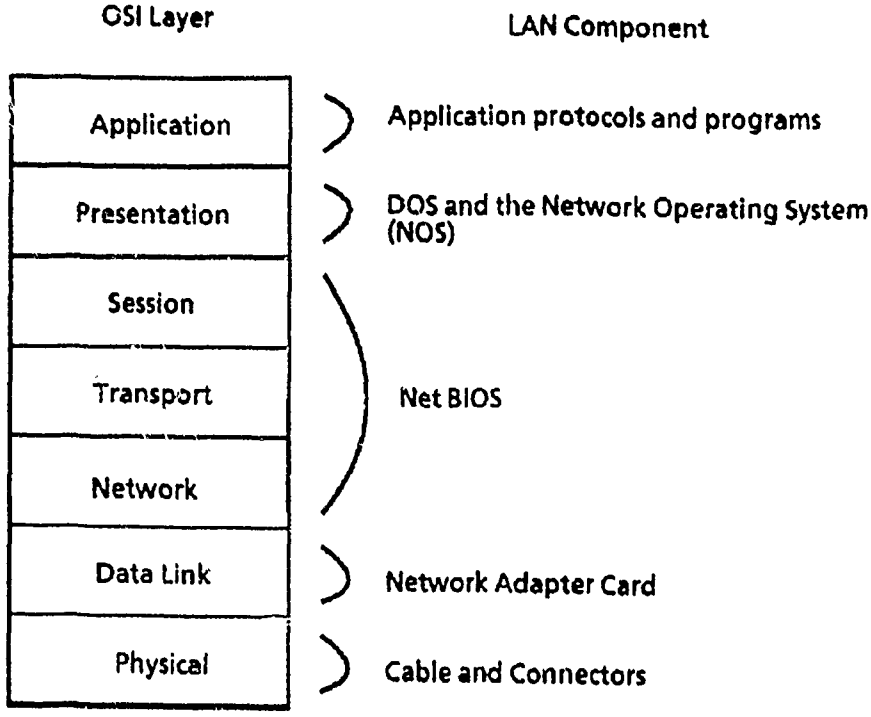


Figure 13. OSI Model LAN Equivalent Layers

tion of existing protocols involves a potentially painful protocol conversion process. If done seamlessly, this process can be painless. Gateways may provide protocol conversion between different layer protocols, fragmentation, reassembly, and network access authorization checks [Ref. 7: p.4-15]. This conversion can be accomplished in either protocol- or service-based ways as follows:[Ref. 11]

1. OSI Pilots

These prototype systems provide a testbed from which to subject a solution to operational testing conditions before implementing the actual system. This testing approach fields a system which hypothetically has the major defects worked out of it. The NIST has developed an In-situ application-gateway for this purpose, and the MITRE Corporation has developed a staging application-gateway. Both gateways are discussed later in this chapter.

2. Mixed Protocol Stacks (Dual Stack)

This is a protocol-based approach where two sets of protocols are kept on the gateway. This approach has two likely disadvantages[Ref. 11: p. 521]:

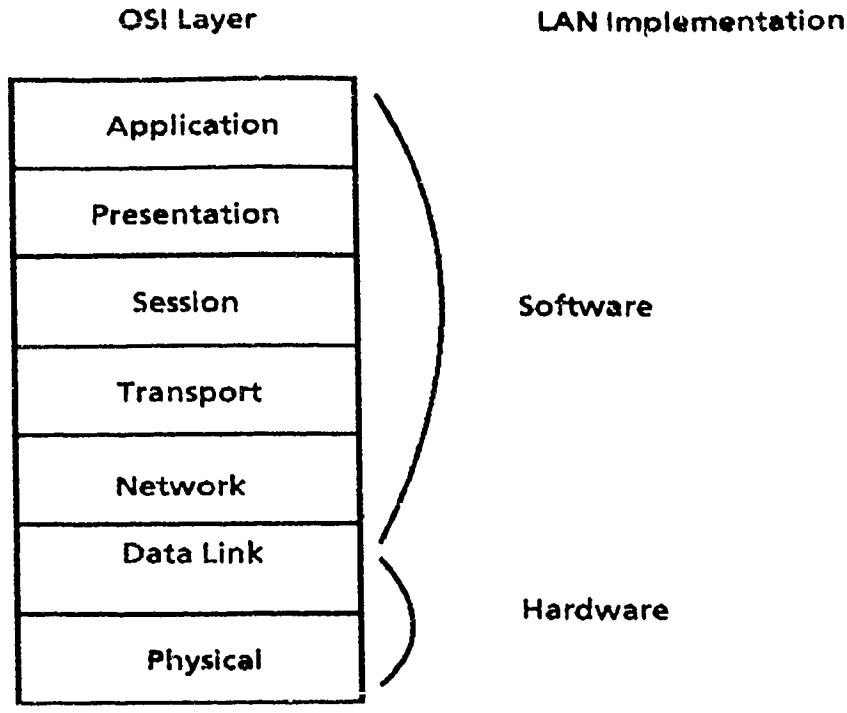


Figure 14. OSI LAN Equivalent Layers

- Lack of an infrastructure to support a second set of protocols. The system may not be capable of maintaining a new set of protocols due to software maintenance.
- Lack of additional hardware capacity. The gateway may lack sufficient memory or space for hardware modifications.

Figure 16 on page 29 shows a diagram of a mixed protocol stack [Ref. 18].

3. Gateway

a. Application-Gateway

The most common use of this strategy is for store-and-forward applications. Protocol conversions in these applications can involve loss of information during the conversion process, depending on the degree of protocol mismatch between the protocols being converted at the gateway. For example, text oriented message exchanges ... the Internet are permitted through SMTP, while X.400 (MHS) offers a multi-media mail facility. Gateways in this context, prov'e a connectivity solution, but a poor interoperability solution due to the loss of information during the conversion process [Ref. 11: p. 537]. Figure 17 on page 30 shows an example of an application gateway[Ref. 11: p. 537].

Comparison Of Layering In Major Architectures

Layer	OSI	DoD Internet		SNA	Decnet
7	Application	TELNET		End User	Application
6	Presentation	FTP		Presentation Services	
5	Session	SMTP		Data Flow Control	(none)
				Transmission Control	
4	Transport	Transmission Cntrl (TCP)		Path Control	Network Services
3	Network	Internetwork (IP)			Transport
		X.25 level 3	1822 level 3		
2	Data Link	Data Link (HDLC)	Data Link (HDLC)	Data Link Control (SDLC)	Data Link Control (DDCMP)
1	Physical	Physical	Physical	Physical	Physical

Figure 15. OSI Layer Comparisons for Major Architectures

(1) Staging Application-Gateway. This protocol conversion process is better suited for message transfers. A file is transferred in a store- and-forward fashion. That is, files are received completely at each node before passing the file along the path to the next node.

(2) In-situ (on-the-fly) Application-Gateway. This gateway has higher granularity than the staging Application-Gateway, and is still a store-and-forward gateway. This gateway is better suited for file transfers, as it has a high throughput rate. The tradeoff for this speed are imperfect mappings across the gateway.

b. Service-based Gateway

These gateways achieve conversion by emulating the services from different protocol suites. For example, a transport- service suggests end-to-end OSI applications running between networks. This is a hybrid solution between a Dual-Stack Gateway and an Application-Gateway.

4. Ultimate Goal

There is no difference in quality of mappings across either types of application-gateways. The difference between the two gateways is obvious when the

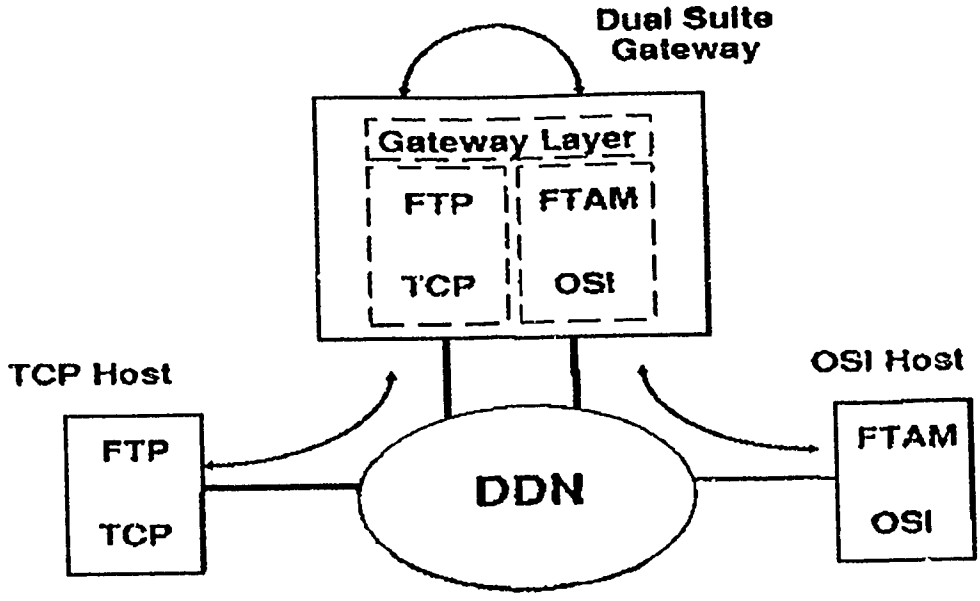


Figure 16. Dual Stack Model of Application Gateway

service provided by either file transfers or message delivery is considered by the user. Users are not interested in the protocol suite that handles their messages. Rather, the Computer Based Message System should provide services that the intended users are comfortable with using.[Ref. 11]

C. MESSAGE PROTOCOLS

1. JANAP-128

AUTODIN uses ASCII computer code to send messages using JANAP-128 message format. These messages consist of the following main components:[Ref. 3: Appendix C]

- Header
- Ending

Appendix C shows the fields of JANAP-128.

2. RFC-822

DDN uses the RFC-822 message format within its SMTP protocol for sending E-Mail messages. In DMS, this would correspond to individual messages. RFC-822

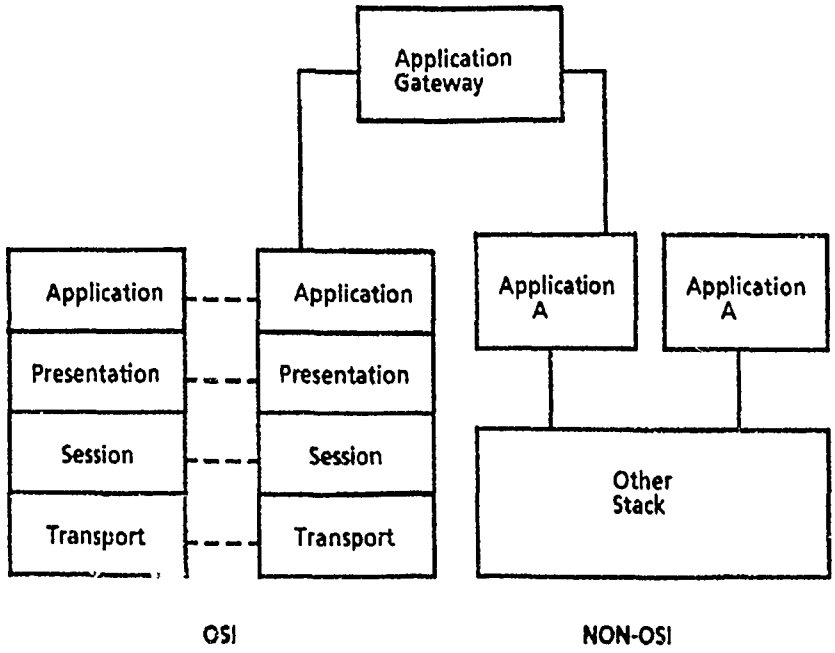


Figure 17. Model of Application Gateway

format is a memo-type format, and is very flexible in the services that this format can provide to the user. These messages consist of the following components[Ref. 5]:

- Header
- Body
- Ending

Figure 18 on page 31 shows the RFC-822 message fields[Ref. 19: p. 591].

3. X.400 (1984)/Message Oriented Text Interchange System (MOTIS)

CCITT developed the X.400 protocol at about the same time ISO developed MOTIS. MOTIS gained such popularity and widespread use that it rivaled X.400. CCITT modified the X.400 (1984) protocol to be compatible with MOTIS in response to this popularity. Figure 19 on page 32 shows the header fields and message structure of X.400[Ref. 20: p. 166]. The components of these protocols are:[Ref. 21: p. 577]

- Heading
- Body
- Ending

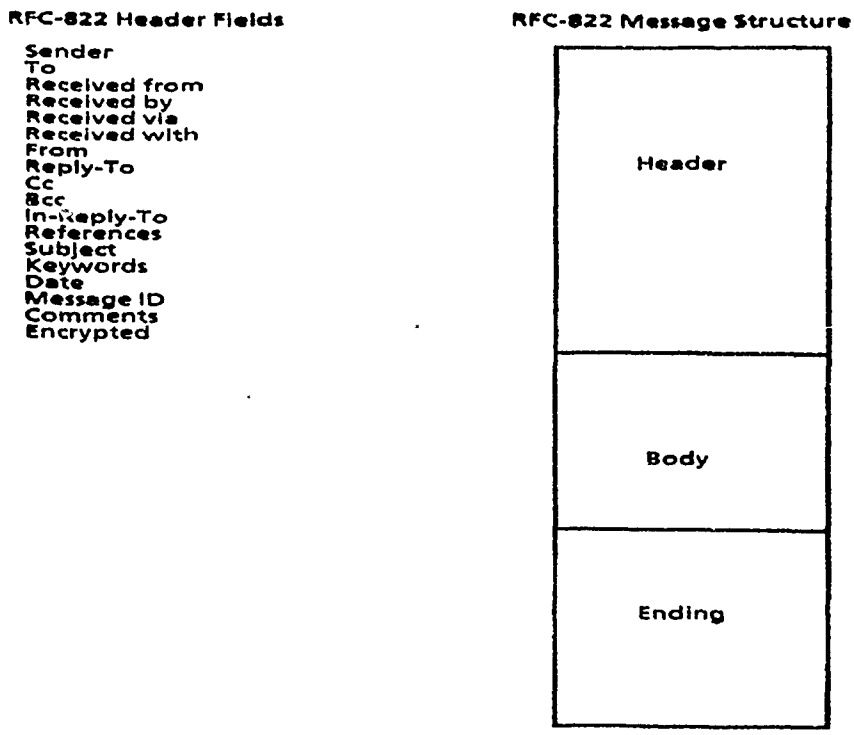


Figure 18. RFC-822 Components

Figure 20 on page 33 shows the functional model of MHS[Ref. 20: p. 166]. Figure 21 on page 34 shows the CCITT X.400 family of standards for MHS[Ref. 21: p. 572].

4. ISO Development Environment (ISODE)

Figure 22 on page 35 shows the ISODE protocol layers in relation to the ISO Model[Ref. 11: p. 387]. This model offers a means by which to use OSI protocols on top of existing Internet protocols. For example X.400 on top of TCP/IP allows use of the OSI application layer protocols with the widely implemented TCP, IP protocols. There is some loss of the full functionality of X.400, but this offers a transition strategy to users who have implemented TCP, IP.

D. DMS MESSAGE CONVERSION PROCESS

1. Baseline

AUTODIN and DDN messages remain largely disjoint during this period. The gap between the DCS and an organizational user is bridged using automation. Existing protocols are used on their respective networks. An ADI is incorporated near the end of this phase. This interface provides a gateway between the two networks for messages

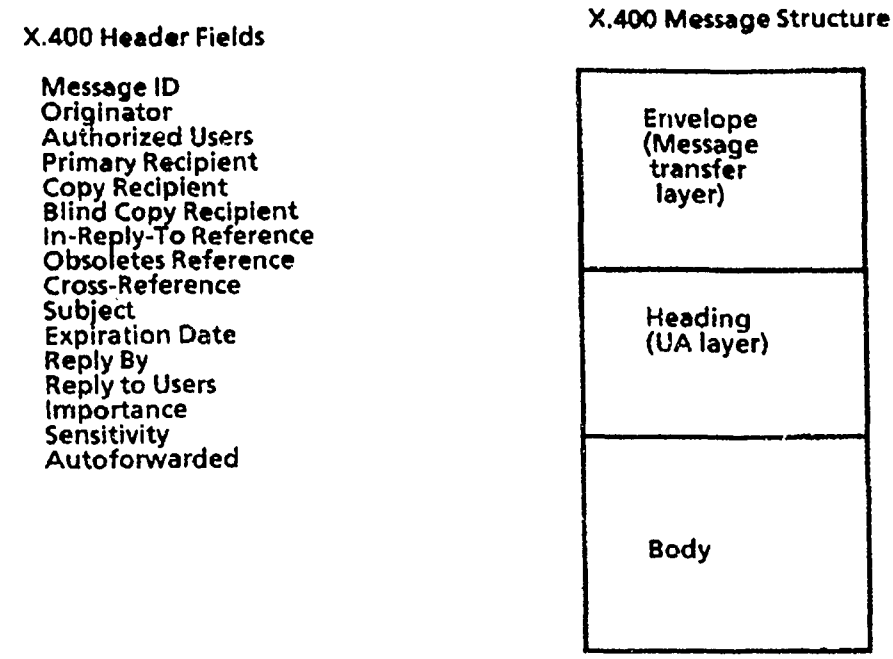


Figure 19. X.400 Components

destined for recipients on the opposite network. For example, a DDN message may contain an addressee who can only receive messages from AUTODIN. The ADI provides the path for the message to reach that addressee directly from DDN[Ref. 22: p. 73].

2. Phase II

A hybrid gateway between dual-stack and application-gateway best positions the users for eventually adopting OSI protocols and exploiting the strengths that OSI offers the user. This approach offers a transition solution to the OSI migration problem. The Navy policy during this period is for Navy users to migrate toward the X.400 protocol. Users who operate OSI applications over existing sublayer protocols would experience less turmoil in the transition to X.400. ISODE provides a possible implementation of this concept[Ref. 23]. In this implementation, X.400 and OSI protocols are running on top of TCP/IP protocols.

3. Phase III

The major components of the existing networks are supposed to begin being phased out during this phase, so experienced users in OSI protocols would experience

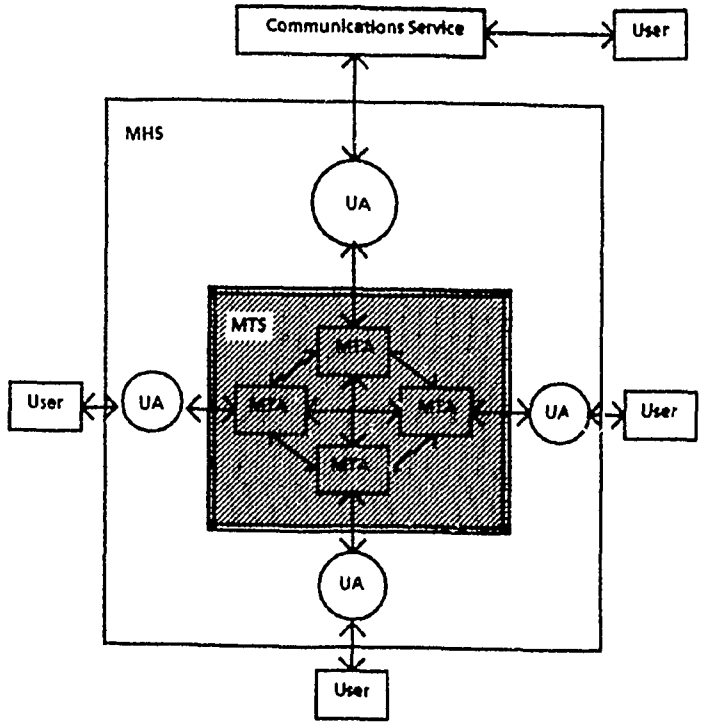


Figure 20. MHS Logical Functionality

enhanced services as the overall network becomes increasingly an open system. OSI applications are expected to be fully developed to the level that Internet protocols are developed today.

E. SYSTEM SECURITY

Chapter II mentioned E^2 and link encryption, but did not discuss the threats to computer security. Figure 6 on page 15 shows a generalized concept of link and E^2 encryption. These two encryption schemes provide the fundamental encryption alternatives [Ref. 24: p. 65]. A means to disguise traffic flow so as to hinder traffic analysis is to use traffic padding, which sends filler messages in between actual messages[Ref. 24: p. 65]. There are two major threats to security, active and passive, as follows [Ref. 24 : p. 70]:

- Passive
  - Monitoring and or recording traffic as it is passed
  - Release of recorded message contents to flood the network

X.400 Family for MHS Protocol Standards

Number	Title	Description
X.400	System Model Service elements	Defines MHS model (UA, MTA); defines interpersonal messages, MTS
X.401	Basic service elements and optional variable facilities	Divides services into requirements; error option; addition option
X.408	Encoded information type conversion rules	Specifies rule for convertin to another format
X.409	Presentation transfer syntax	Defines data structures in transfering messages
X.410	Remote Operations	Define MHS for remote terminals, defines how uses session layer
X.411	Message transfer layer	Specifies protocols at message transfer sublayer
X.420	Interpersonal messaging UA layer	Specifies format for using header and multipart body types
X.430	Access protocol for teletex teminals	Specifies protocol required to support teletex terminals

Figure 21. X.400 Family of Protocol Standards

- Traffic analysis allows reading of addresses from headers to determine location and identity of hosts

- Active - Intrude on the network to alter transmitting data or control signals
  - Denial of message service
  - Masquerade (spoofing)
  - Message stream modification

1. Trusted Guard Gateway (TGG)

The TGG illustrates an attempt to allow limited, controlled communication segments at different levels of security authorizations. It is designed primarily for the DDN to serve different levels of trust and security levels[Ref. 25: p. 5]. In this scenario, it then provides MLS for the DDN.

2. Secure System Design Principles

A secure system must be designed to withstand malicious attacks. Protection mechanisms can deter to a great extent such attacks, and design principles to accomplish that are suggested as follows[Ref. 26: p. 372]:

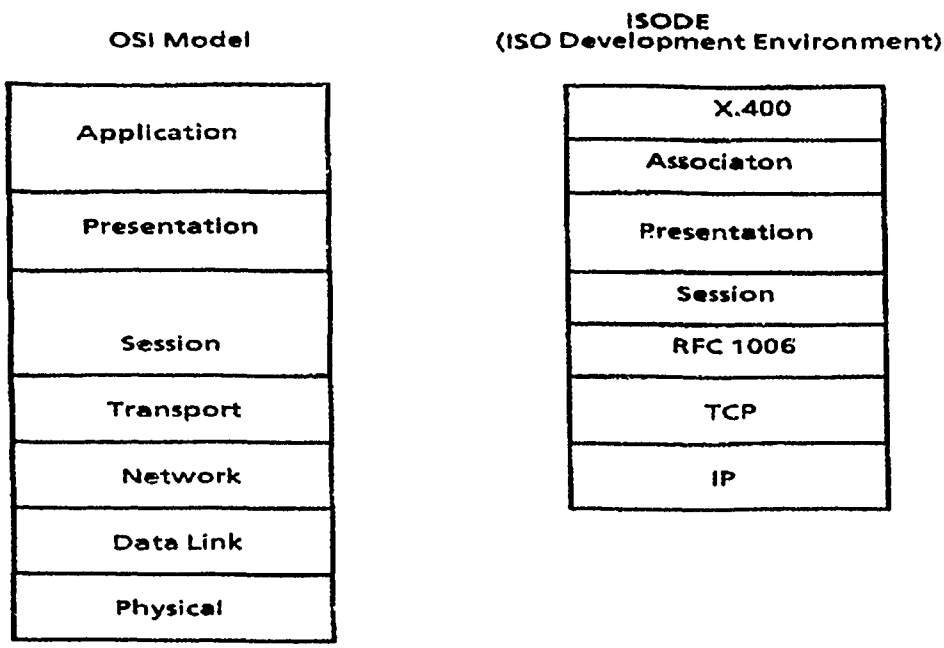


Figure 22. ISODE Protocol Layers Compared to OSI Layers

- Economy of mechanism - Simplest possible design that achieves desired effect
- Fail-safe defaults - Access based on permission rather than exclusion
- Complete mediation - Every access request checked against an access control database
- Open design - Design should not be secret so as to depend on keys, passwords
- Separation of privilege - Two keys to open locks renders a more robust system
- Least privilege - Use least set of privileges to preform a task
- Least common mechanism - Commonality of sharing mechanisms are minimized
- Psychological acceptability - Users comfortable with system and readily use it

E^2 encryption offers the greatest network security, as only the two sharing hosts have the keys to decrypt the message[Ref. 27 : p. 414]. Link encryption provides the supplementary encryption to combat traffic analysis, resulting in a relatively secure network.

F. CHAPTER SUMMARY

DMS represents a messaging philosophy and a protocol suite goal towards which current protocols must reach. This transition to OSI standards must be a gradual and phased operation to preventive excessive turmoil for organizational users. The period of coexistence of Internet and AUTODIN protocols with OSI protocols is expected to last as long as the turn of the century. It makes sense then, to use DDN protocols as an infrastructure until OSI achieves dominance. Users in this environment who are not using DDN must become subscribers to that network, or risk loss of information vital to the operation of their organization.

IV. A PROPOSED MCB DMS IMPLEMENTATION STRATEGY

A. BACKGROUND

The previous chapters have served to show that Marine Corps planners must consider the task of the graceful transition from traditional AUTODIN message systems to DMS and its OSI structure. A graceful transition process is necessary because there should not be any interruption to an organization's operational performance due to this conversion. The revolutionary approach to message systems offered by DMS presents a singular opportunity for the Marine Corps to tailor its message system according to an organization's requirements. The streamlining effect on Command and Control systems with this more effective message system is well worth the effort to implement DMS to its fullest extent.

1. Current Message System Topology

The current AUTODIN system procedures were mentioned in Chapter II. The AUTODIN message system at MCB Camp Pendleton is used as a model for proposing a DMS implementation strategy. There are six major commands aboard MCB Camp Pendleton as follows:

- Commanding General, First Marine Expeditionary Force (I MEF)
- Commanding General, Fifth Marine Expeditionary Brigade (5th MEB)
- Commanding General, First Marine Division (1st MARDIV)
- Commanding General, First Force Service Support Group (1st FSSG)
- Commanding Officer, Marine Aircraft Group 39 (MAG-39)
- Commanding General, Marine Corps Base Camp Pendleton (MCB CAMPEN)

The first five organizations in the above list comprise Fleet Marine Forces (FMF), and the last organization represents Supporting Establishment (SE) organizations aboard MCB CAMPEN. Included in the SE organization list are non-USMC organizations such as Naval Investigative Service (NIS), Naval Hospital, et. al. The SE provides the DCS interface, i.e., AUTODIN connectivity for all MCB organizations through the Marine Telecommunications Center (MTCC). This MTCC has the following components as shown in Figure 23 on page 38[Ref. 28: p. 6-7]:

- Remote Information Exchange Terminal B (RIXT-B)
  - Video Display Unit (VDU)

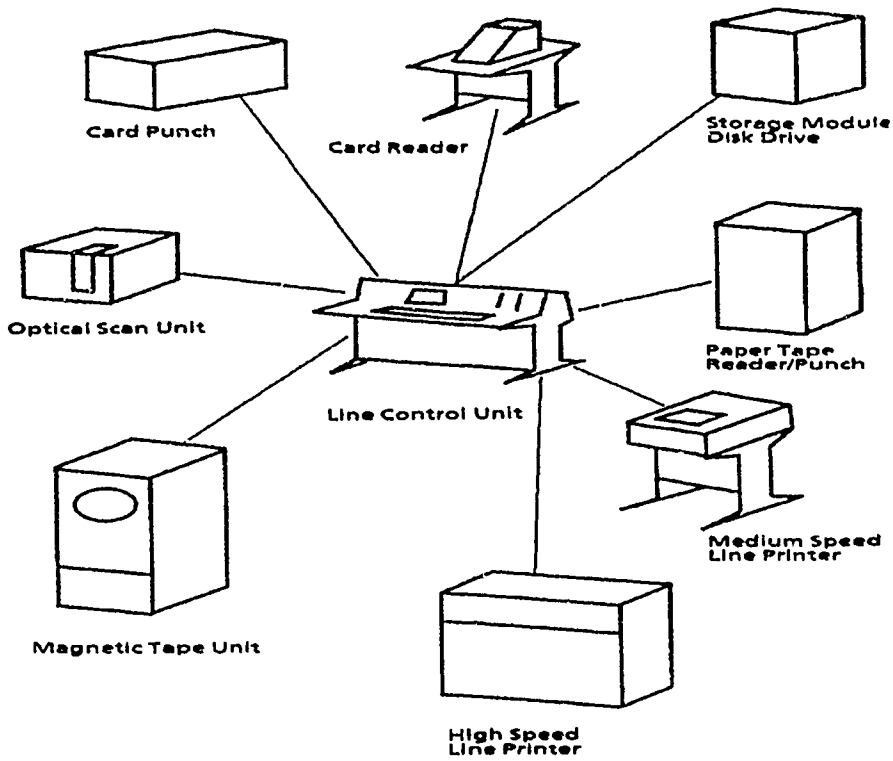


Figure 23. RIXT Components

- Optical Character Reader (OCR)
- Paper Tape Reader'Punch (PTRP)
- High Speed Line Printer (HSLP)
- Medium Speed Line Printer (MSLP)
- Magnetic Tape Unit (3) (MTU)
- Storage Module Disk Drive (SMDD)
- Card Reader
- Card Punch

- Xerox 975 Copiers
- Model 28 Teletypewriters
- KG-84A Cryptographic Devices

This MTCC is homed off of the Local Digital Message Exchange (LDMX) at the Naval Communication Station (NAVCOMMSTA), San Diego. The base encompasses a large land area (roughly 15 miles by 15 miles) to accommodate training exercises. This results in widely dispersed organizational areas (camps) among these training

areas. There are 11 major camps scattered on MCB CAMPEN, the furthest located approximately 15 direct miles from the MTCC. Figure 24 on page 40 shows the dispersion of the organizations on MCB Campen.

The network required to interconnect these dispersed organizations is consequently expansive. The existing transmission medium o MCB CAMPEN is composed primarily of twisted pair telephone wires, although microwave radio T-1 links comprise the backbone of this network, with some fiber-optic cables as tributaries.

OTC service with the MTCC in this environment involves major round-trip delays for all organizations except for the headquarters of the seven major organizations. Delays in the extreme of an hour are normal for the most distant organizations.

Banyan VINES has been declared as the Network Operating System (NOS) for Marine Corps' LANs since April 1989[Ref. 29]. This NOS is discussed later in this chapter.

2. Scope of this chapter

This chapter focuses on the DMS Phase I implementation issues facing Marine Corps users. The LAN organization of MCB CAMPEN is briefly discussed, but the focus of attention will be on the LAN for a senior FMF organization, such as I MEF. This organizational LAN serves as a model from which to show a proposed topology from which to extend automation from the DCS to an Office Automation System (OAS). Such issues such as connectivity, message dissemination, releasing officer certification, network security, and message text format will be examined within this chapter. The major organizations generate the most messages, as well as receive the most message traffic among those organizations aboard MCB CAMPEN. Any Marine Corps topology must obey DOD and Navy regulations, so that the Navy BITS and NDCCA requirements are examined within the context of applicability to Marine Corps functionality. Ultimately, the implementation topology proposed in this chapter is intended to be translatable into tactical operations where DCS interoperability is required, in terms of message systems.

B. MESSAGE SYSTEM TOPOLOGIES

1. MCB Information Transfer System

The cable plan for MCB CAMPEN consists largely of twisted pair telephone wire, but with an implementation of T-1 microwave radio backbone media and fiberoptic cable tributaries. Additionally, MCB CAMPEN has a digital telephone switch which postures MCB CAMPEN well for an integrated voice and data environment within

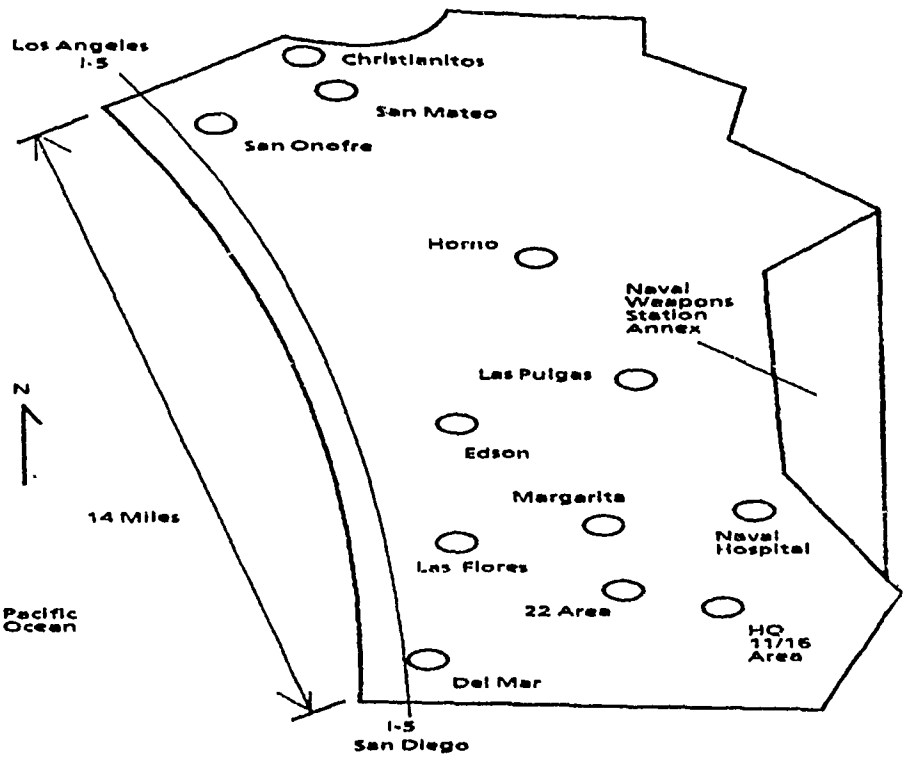


Figure 24. Geographical Representation of MCB Camp Pendleton Units

ISDN. The overall cable plan for MCB CAMPEN is shown in Figure 25 on page 41[Ref. 30]. The DMS Target Architecture and Implementation Schedule (TAIS) plans for a target implementation date for ISDN for 2010 with the ISDN service access structure as shown in Figure 26 on page 42[Ref. 31 : p. 70].

2. Navy Data Communications Control Architecture (NDCCA)

A Marine Corps DMS implementation plan must conform to the Navy NDCCA. This architecture provides the safeguards and features necessary to protect classified information. The electronic connection to the DCS makes the endpoint a part of the DCS, and subject to DCA certification. Ideally, a multilevel secure (MLS) LAN would allow the MCB CAMPEN LAN to provide a communications network as a backside LAN to the DCS gateway. Figure 27 on page 43 shows the NDCCA elements necessary to protect classified and sensitive information[Ref. 32: p. 7]. E^2 encryption through SDNS and link encryption through the KG-84A provide a significant barrier to malicious alteration of message traffic.

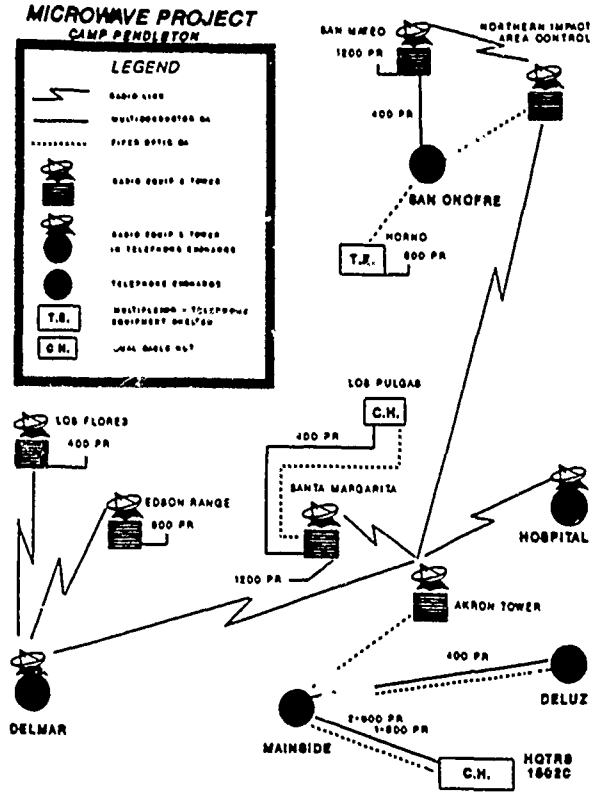


Figure 25. MCB Camp Pendleton Cabling Plan

3. MCB CAMPEN Network Management Center (NMC)

A NMC encompasses the following functions or disciplines[Ref. 33: p. 319]:

- Operations
- Administration
- Maintenance
- Configuration management
- Documentation training
- Database management
- Planning
- Security

The network management functions include statistics collection and also, possibly access control. This function could allow who can communicate with whom and administer issuing of session keys for encryption. Each organization should have an Information Systems Management (ISM) function to provide local and near-term computer training and planning. The NMC would provide services of LAN management

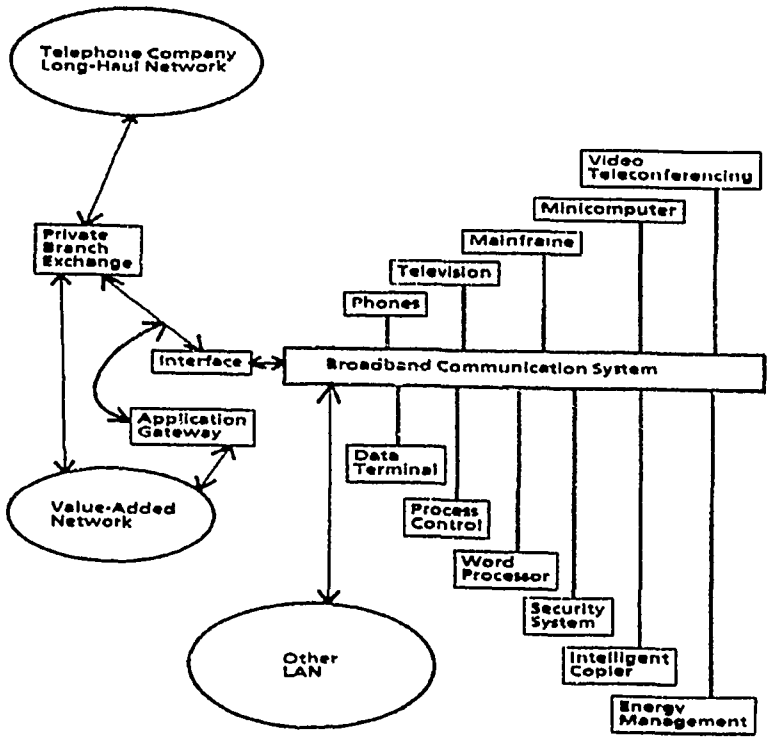


Figure 26. ISDN Service Access Requirements

and connectivity. The elements of this topology translates directly into a tactical environment.

C. MCB CAMPEN DMS BASELINE TOPOLOGY

The previous chapter dealt with protocol issues at the internetworking level. The Marine Corps implementation of LANs to the Banyan VINES Networking Operating System (NOS) is required to operate within a generalized protocol structure as shown in Figure 13 on page 26. The VINES network should be Internet (DDN) compatible in consideration of the requirement to connect with DDN for purely computer to computer messages. The VINES NOS is used as a means to explain the MCB CAMPEN overall topology as explained below:

1. Banyan VINES

Banyan VINES, by virtue of its virtual network topology, has an inherent flexibility not found in many NOSs. Topology in this sense refers to the way in which the nodes of the network are interconnected[Ref. 33: p.53]. VINES supports a wide range of LAN mediums, and when acting as a Network Server, can function as a bridge with

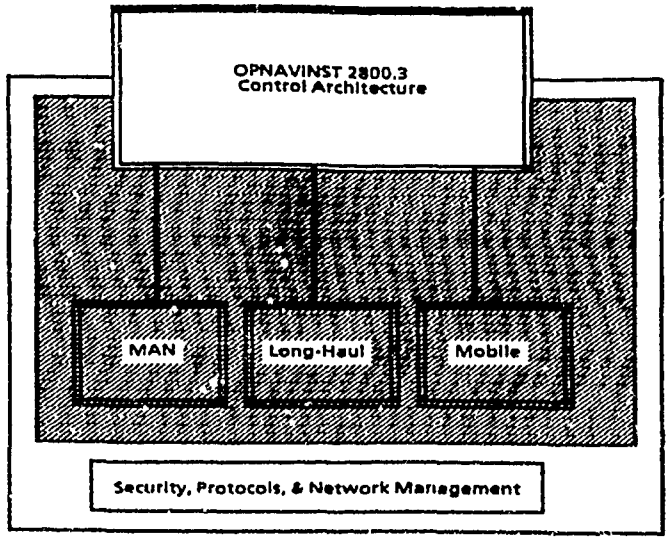


Figure 27. NDCCA Environment

up to four distinct mediums [Ref. 34: p. 90]. This requires an applicable Network Interface Card per different configuration.

2. Versatile access control

VINES' global naming scheme (distributed directory services) allows tracking of network users and resources by operating system. The transparent nature of this scheme allows users of large, multiserver LANs to access resources on a LAN without having to know where the resources reside[Ref. 35: p. 37]. Security is enforced at several points in VINES as follows[Ref. 36: p. 72]:

- Server console operation
- Server-to-server internetwork data exchange
- Service access
- User network login

The user profile configured by the Network Administrator serves to segregate levels of users on a multilevel service. VINES,286 security is focused at three levels as follows[Ref. 37: p.72]:

- Username protection
- Password protection
- Directory security rights
  - Control access

- Modify access
- Read access
- Null access

3. Organizational LAN topology

Organizational LANs, as users of the Banyan VINES network have three main choices in topologies:

- Bus
- Ring
- Star

Figure 28 on page 45 shows these generalized topologies, and additionally, a combination of ring and star, ring-star. A ring topology serves the best interests of an organization for the following reasons[Ref. 33: p. 91]:

- The transmitted signal is regenerated at each node
- Greater coverage is possible
- Fault isolation and recovery is simple
- Addition and deletion of nodes is relatively easy

The unidirectional nature of ring topologies have additional favorable attributes[Ref. 38: p. 12]:

- Simplified message routing since only one routing path is possible
- There is the possibility for low capital investment, with cost proportional to the number of users or interfaces
- The possibility of high throughput exists since more than one message can be in transit at once.

Token ring topologies allow each node to have equal access, also. This managed access assures fairness, and also allows a precedence system by which a node can have guaranteed access rights to transmit messages on the network. Rings provide the best performance for networks with a small number of nodes operating at high speeds over short distances [Ref. 38: p. 13].

4. DDN implementation

The software of VINES 3.0 enables the NOS to act as a TCP/IP bridge [Ref. 39: p. 5]. An application gateway is needed, however, if the mail software is to be used for non-Banyan addresses. Subscribing to the DDN enables greater interservice communications and conforms to the DMS TAIS, as mentioned earlier. Figure 29 on

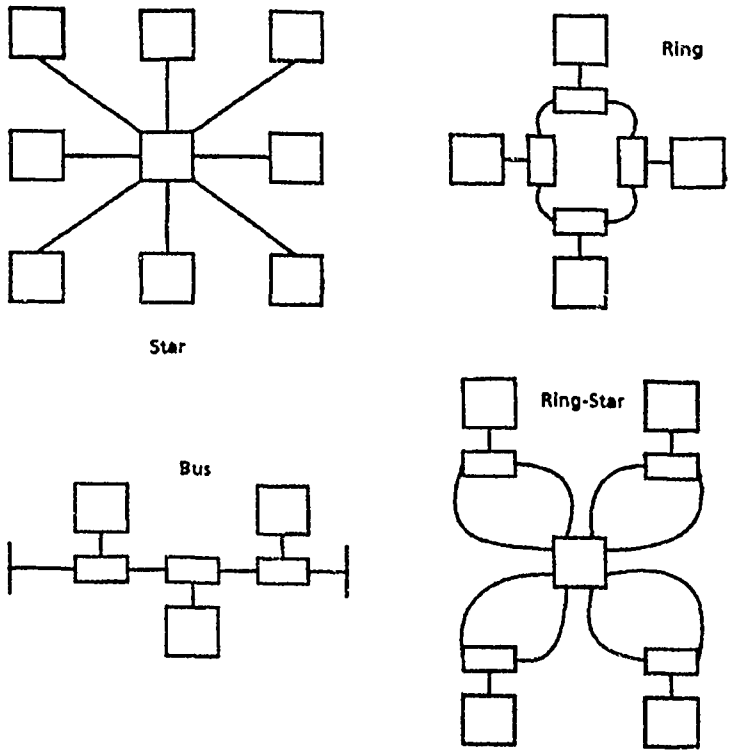


Figure 28. Representations of LAN Topologies

page 46 shows the DMS Baseline target architecture for MCB Campen. An SMTP mail system, and full compatibility with the Internet protocol suite is necessary in preparation for the DOD migration towards OSI standards.

5. MTCC configuration

The MTCC should provide automated services during this baseline period as shown in Figure 30 on page 47. This configuration enables organizations to process their AUTODIN messages via diskette media vice DD-173 paper media.

The Message Generation Software-2 (MGS2) software developed by Naval Regional Data Automation Center (NARDAC) Norfolk, Virginia offers a user friendly message processing software in Message Text Format (MTF) (see Appendix D for MTF format). PCMT hardware, software, and Bus Interface Unit (BIU) are needed for the MTCC to provide the basic automated message services to MCB CAMPEN organizations. DMS Phase I configurations provide more robust automation for the major organizations.

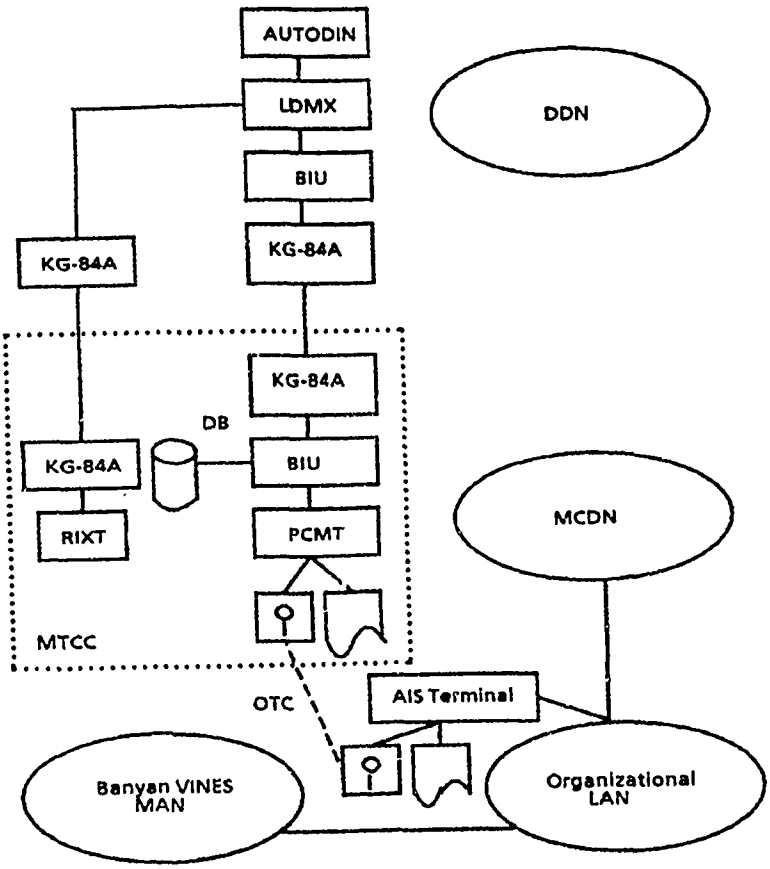


Figure 29. MCB Baseline Configuration

D. MCB CAMPEN PHASE I TOPOLOGY

The MCB Campen Phase I topology is reasonably attainable with available equipment. This topology is suggested in Figure 31 on page 48. The BIU and Gateguard software are necessary for those organizations who possess microcomputers already. Gateguard and its role to the organization is discussed below.

1. LAN organization

Banyan VINES must be a MLS LAN in order to connect all organizations on MCB CAMPEN to the DCS gateway via their MCB CAMPEN LAN. The differing levels of users according to their authorizations are kept segregated through a Trusted Organizational User Agent (TOUA). The absence of a TOUA creates a situation wherein the network is operating at level as high as the lowest authorization of any user on the network (system high). Link encryption through KG-84A or STU-III make such

MESSAGE TELLER TERMINAL

(MTT)

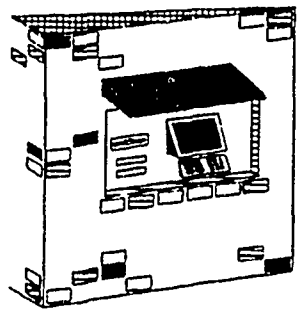


Figure 30. MTT Configuration

a system possible. In such a scheme, each node for the link encryption is a weak point, as the message traffic is uncovered at this point.

2. Personal Computer Message Terminal (PCMT)

The PCMT is the communications terminal with software that is designed primarily for communicators, due to the AUTODIN- specific jargon and procedures that it uses. Additionally, the terminal is a replacement for the following equipment[Ref. 40]:

- AUTODIN Mode V
- DC 2000
- SRT RIXT

Figure 32 on page 49 shows the minimum PCMT configuration. This system provides the processing capabilities and storage for the Message Teller Terminal.

3. Message Teller Terminal (MTT)

The MTT provides an automated replacement to the OTC service for handling diskettes. Manual diskette OTC service is still retained as a backup to a MTT failure.

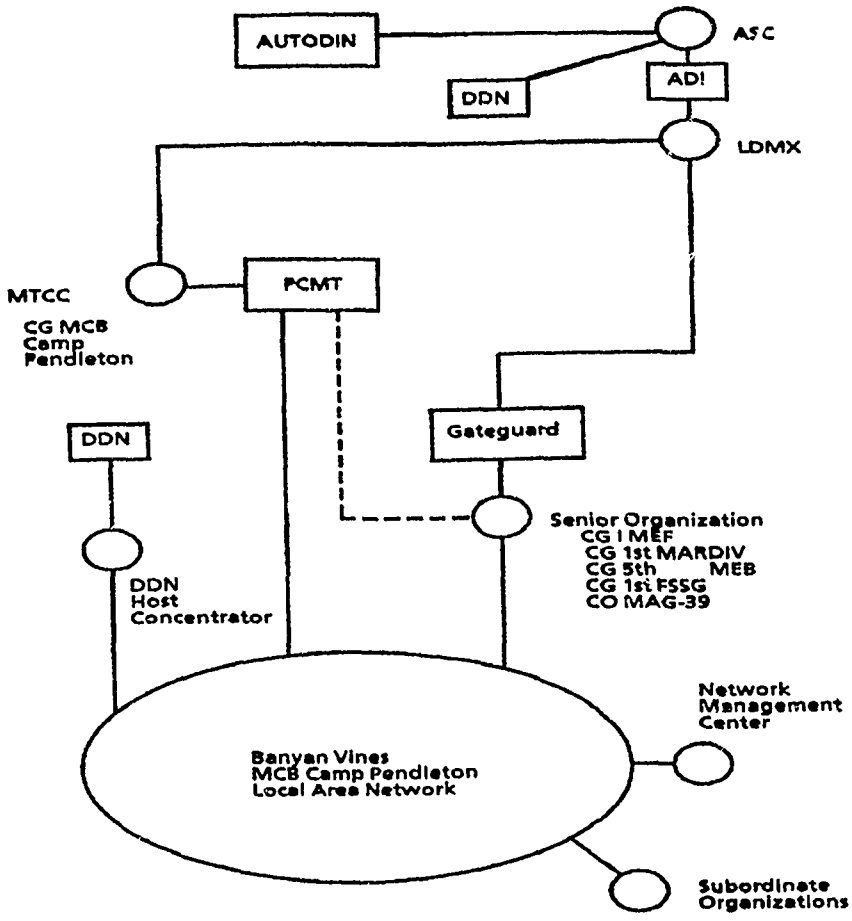


Figure 31. MCB Phase I Implementation

It is designed to streamline an old system which is paper based, slow, manpower intensive, highly prone to human error, and does not ensure accountability[Ref. 41].

a. MTT components

The MTT components are as follows:

- Video Display Unit (VDU)
- Printer
- Diskette Drive
- Magnetic Card Reader
- Fingerprint Reader
- Keypad

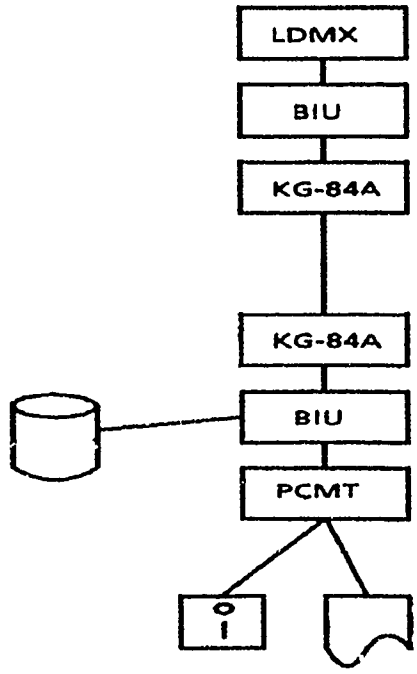


Figure 32. PCMT Minimum Configuration

Each MTT session is videotaped for security. This videotaping combined with the fingerprint identification and magnetic card (Subscriber Access Card (SAC)) form a positive courier identification system. Figure 33 on page 50 shows the configuration at the MTCC with the MTT installed as an OTC device.

b. MTT operations

The MTT is designed to process 1,500 messages daily. All messages delivered to the MTT must be prepared in accordance with NTP3_, Annex C. A courier must enter the CRC number and diskette volume identification from the DD 1392 accompanying the diskette from the organization. Once the messages are successfully entered into the MTT system, a DD 1392 from the MTT is printed as a receipt for the messages. The courier's SAC provides more than the courier's identification, it also provides the organization's RI.

c. MTT reports

Audit trails are integral parts of the system, both visual and hard copy. The following reports provide these audit trails:

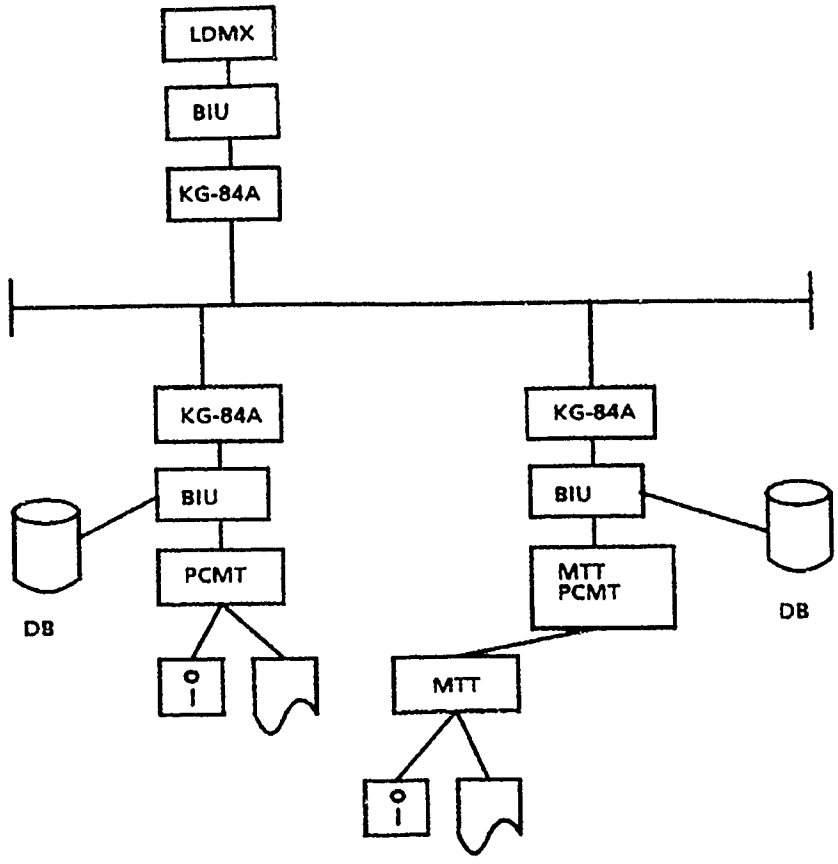


Figure 33. MTT Configuration for OTC Service

- Message Accountability Report
- Log Summary Report
- Diskette Summary Report
- Device Status Report
- System Restart Report

4. Gateguard

The Gateguard system provides an organization with the AUTODIN Gateway Terminal (AGT) for interfacing the organization's LAN with AUTODIN[Ref. 42]. Figure 34 on page 51 shows the overall configuration with the MTCC and units with Gateguard.

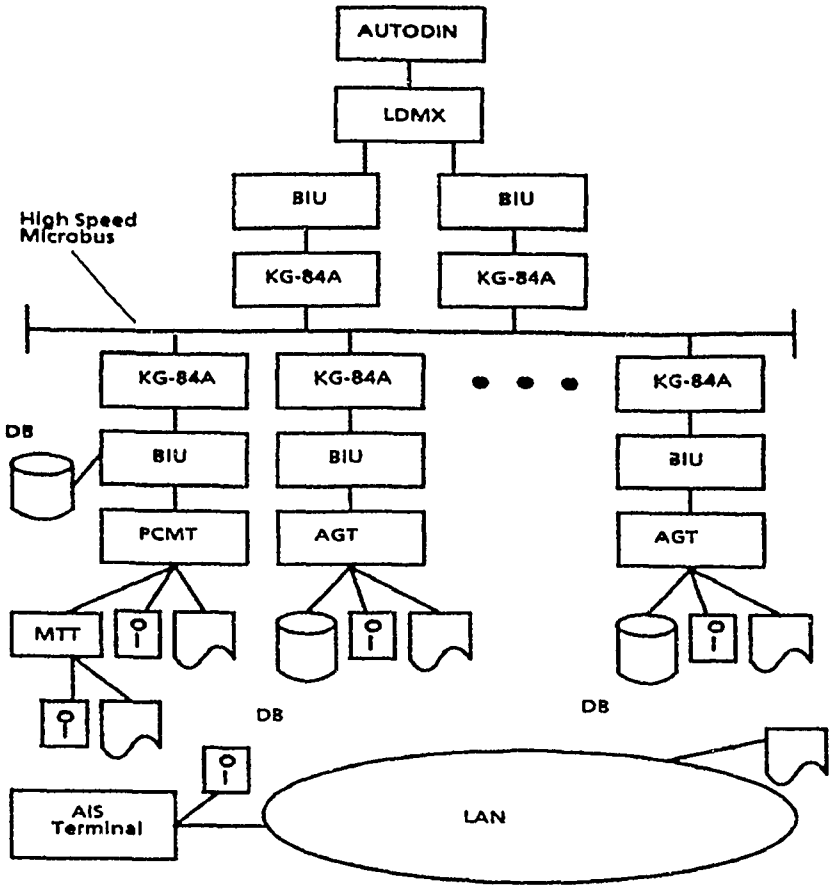


Figure 34. Gateguard Subsystem Implemented on MCB

a. Components

The components of Gateguard are as follows:

- AGT
- Guard Device (BIU)
- Cryptographic equipment for links outside of secure spaces
- Modems (for cable runs exceeding 50 feet) at 2400 Baud
- Printer

b. System requirements

The Gateguard system requires the following components:

- IBM AT (or compatible)
- Color Enhanced Graphics Adapter (EGA) monitor

- Two Megabytes (MB) of Random Access Memory (RAM)
- One mass storage disk drive with a capacity of at least 30 MB
- One 5.25 inch 360 Kilobytes (K) diskette drive
- Two synchronous, RS-232C communications ports

c. Operations

Figure 35 on page 53 shows the operations of Gateguard[Ref. 40: p. 5]. Delivery to the AGT constitutes delivery of the message to the intended recipient. Any system attached electronically to the AGT is then a component of the DCS, and subject to DCA certification. These two factors are very important in determining whether a LAN is to be attached directly to the AGT. A TOUA is necessary to provide the MLS capability of a LAN. The alternative to a TOUA is to operate the LAN in a system high mode, where all authorized users must have an authorization at least equal to the highest classification of the information handled over the LAN. An air gap wherein diskettes are physically transferred from an AIS to the AGT safeguards against jeopardizing the DCS interface. The Guard device (BIU) has restrictions built into the Read Only Memory (ROM) according to the highest capability authorized for the organization to prevent attempts to operate beyond authorized capabilities for that organization. This system is designed to handle up to 2,000 messages daily[Ref. 42: p. 17]. Figure 36 on page 54 shows the diskette media operations between AUTODIN and OAS environments[Ref. 40].

5. Message Processing System

The message processing system serving the MCB organization must provide an automated system of accessing messages for all users from the organizational database. The Message Dissemination System (MDS) must preserve the integrity of incoming messages from unauthorized alterations. A Write Once Read Many (WORM) disk drive provides a storage media of high capacity which also accomplishes this objective. The Navy MDS is designed with the following objectives[Ref. 40: para 2.2]:

- To eliminate the current manual message dissemination procedures which require Navy TCC and/or organization message reproduction and courier service
- To operate at the system high level of the organization's LAN and ADP systems
- To require that all user terminals are IBM PC compatible
- To implement File Server and user terminal software as POSIX and MS-DOS compatible
- To provide file transfer of messages formatted in accordance with CNTCNOTE 2300.X

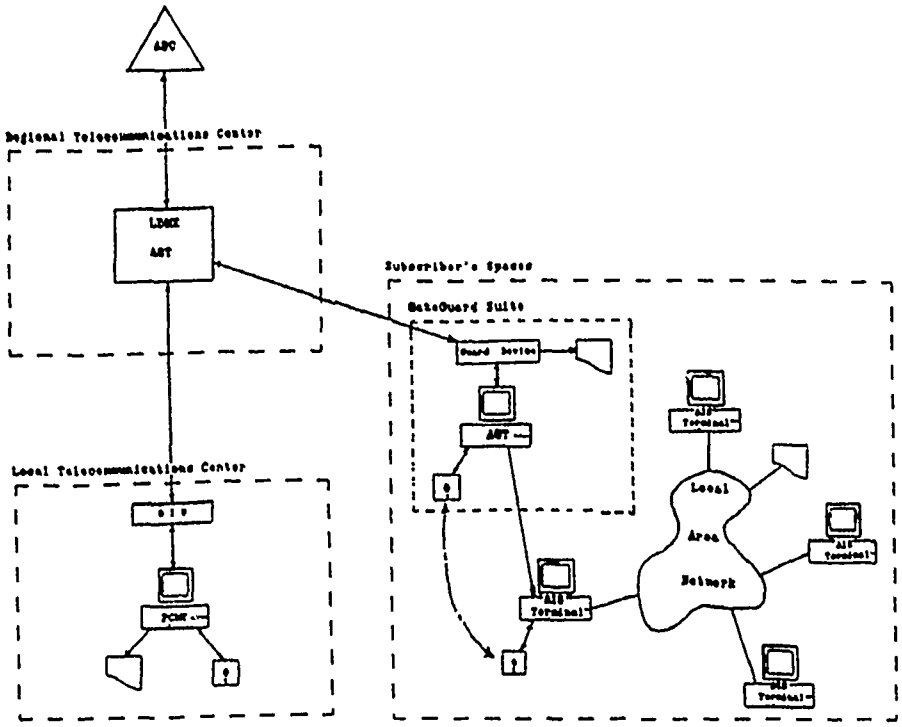


Figure 35. Gateguard Operations

- To use X.400/X.500 compatible design considerations permitting upgrade through operating/network systems enhancements
- To use Commercial Off-The-Shelf (COTS) equipments and systems software to take advantage of technology advancements in the area of office productivity
- To use NARDAC Norfolk MGS2 for user preparation and processing CNTCNOTE 2300.X formatted files
- To migrate using COTS and NDI evolutionary implementations to the GOSIP

a. MDS Operations

(1) Organizational Messages. An organizational user would prepare his message using a MGS-2 like software, resulting in a MTF message. The DD 1392 shown in Appendix D would accompany the message to a Releasing Officer's position for transmittal. In this context, only those terminals used by Releasing Officer's would be used for transmitting messages. All others on the LAN would have receive only access to the AUTODIN Gateway Terminal (AGT). Outgoing messages would thus be controlled while allowing greater organizational-wide access to the database. Banyan

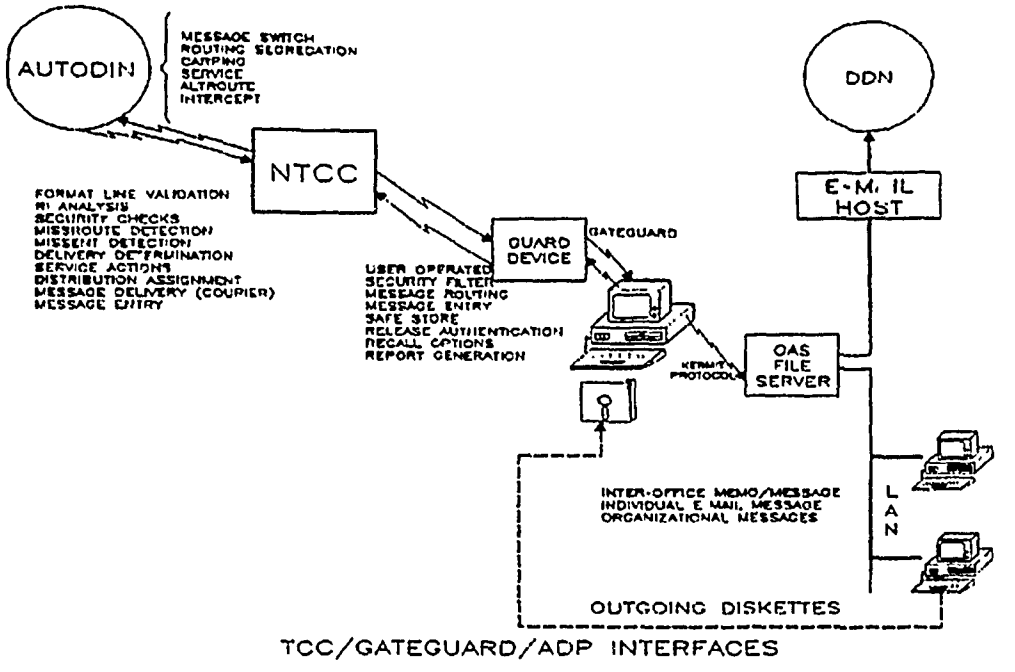


Figure 36. Gateguard Electronic Transfer Operations

VINES allows those users thus authorized to transmit messages, independent of the devices they are located on within the LAN.

(2) Individual Messages. Organizational users would be able to send messages within their LAN or the MAN but require DDN access to send individual messages to interservice or interbase addresses. The Marine Corps Data Network (MCDN) provides this service only within Marine Corps commands, although this is a global service (the MCDN network is shown in Figure 37 on page 55). The Banyan E-mail system provides LAN, MAN E-mail, and with a protocol converter, could provide DDN messages with an Application Gateway as described in the previous chapter.

(3) User Interface. Providing a menu within the E-mail systems offers an easy interface with the user. The Network File Server (NFS) and Network Server (NS) would provide the coordination necessary for E-mail services. A NS that is general purpose server, i.e., is a PC used as a server provides a flexibility to withstand network failures. If such a server fails, then another PC could be used to substitute for the disabled server to restore the network.

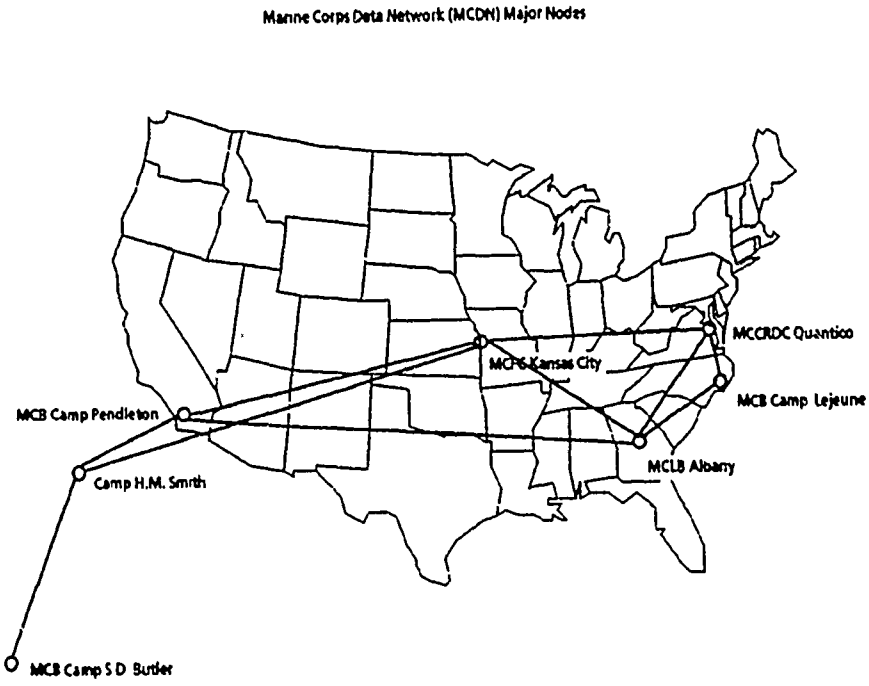


Figure 37. MCDN Topology

6. DDN Access

DDN access is required for those organizations who wish to send individual messages during the Baseline and Phase I periods. Additionally, data pattern message traffic is required to be sent by DDN vice AUTODIN, as mentioned earlier in this paper. Organizations have a great need for DDN access in this environment to communicate with interservice users.

a. DDN Components

DDN access consists of the following standard components[Ref. 7: p. 5-16]:

- Terminal Access Controller (TAC)
- Network Access Components (NAC)
  - Terminal Emulation Processor (TEP)
  - Mini-Terminal Access Controller (Mini-TAC)
  - Host Front End Processor (FEP)

Up to 46 dedicated lines can be connected to a TAC with 16 possible dial up lines[Ref. 7: p. 5-18]. There are three methods of attachment to the DDN as follows:

- Terminal attachment through a TAC
- Host attachment
- Host attachment through a LAN

The TAC provides the terminal handling logic for controlling the terminal and the communications logic for setting up connections across DDN. Attachment through a LAN provides a cost-effective approach by giving all of the LANs hosts logical DDN access[Ref. 43: p. 105].

b. DDN Performance

The DDN enjoys a large installed user base, and yet provides excellent datagram service. A host with the Transmission Control Protocol (TCP) installed experiences undetected Bit Error Rate (BER) of less than 2.9×10^{-10}[Ref. 7: p. 6-3]. SMTP is used to transfer mail, based on the RFC-822 mail format, described in the previous chapter. The characteristics of SMTP are[Ref. 7 : p. 8-25]:

- SMTP is used to transfer mail reliably and efficiently
- Destination host and destination mailbox name, e.g., name@host
- Reverse-path, i.e., who the mail is from; return route
- Forward-path, i.e., who mail is to; source route

E. CHAPTER SUMMARY

This chapter has provided a topology for a MCB organization to gain connectivity both for Organizational and Individual messages through an Office Automation System (OAS). The Gateguard subsystem provides an electronic link to transmit and receive AUTODIN (Organizational) messages, and DDN provides a means to transmit and receive E-mail (Individual) messages. The connection of an OAS is predicated upon operating the system with enough DCA-certified safeguards to protect the information on the system. The KG-84A provides an approved link encryption device for communicating with the AUTODIN system, and the STU-III promises to provide a more widely available encryption device. The MTCC provides a contingency route for an OASs outage through the OTC diskette capability. This capability provides a means for other organizations who cannot operate an electronic link to communicate via diskettes. The enhancements to message communications through this implementation are significant when compared to the traditional AUTODIN-style message communications. The complete transition to DMS offers a tremendous increase in communications effective-

ness as the need for protocol conversion is reduced, and there is a greater utilization of the OAS for all messages.

V. SUMMARY AND CONCLUSIONS

A. SUMMARY

DMS terminology and concepts were discussed in the first chapter along with the current AUTODIN message system procedures. This provided the contrast in procedures and capabilities between DMS and AUTODIN. The DMS TAIS specifies an implementation schedule for DMS, and this schedule was discussed in the first chapter. The second chapter discussed the protocol issues regarding transition from existing protocols to the OSI protocol suite used in DMS. The gateway which provides the protocol conversion was discussed in this chapter to highlight existing protocol structures and to provide a basis for the succeeding chapter. Conversion and convergence issues were discussed in this chapter, as the DDN protocol suite is expected to coexist with the OSI protocol suite for an extended period until total conversion to OSI standards is accomplished. The next chapter built on the concepts of the previous chapters to propose a topology for a MCB to implement DMS, using MCB Camp Pendleton as a model. PCMT and Gateguard were discussed in this chapter to suggest a means for accomplishing this DMS implementation. This chapter proposed that those Marine Corps organizations who are not DDN users must become subscribers if such connectivity is required. The MCDN provides such service within the Marine Corps, and this chapter suggests that the MCDN must be converted to DDN service to comply with DOD directives.

B. CONCLUSIONS

1. Topology

The MCB should use the Gateguard system to automate the message system process. The MTCC should install a PCMT and MTT to enable OTC service for common message service, and as a backup to AIS outages. Link encryption must initially be provided by the KG-84A, and eventually the STU-III will provide the link encryption to a greater organizational base. The LAN/MAN would operate at the system high level until a MLS network can be adopted through SDNS encryption methods.

2. DDN Access

MCB organizations are required to become DDN users for data pattern traffic. They should become DDN subscribers as a logical step towards implementing DMS. DDN access provides individual message access in the near term, as well as a data pat-

tern traffic medium. This DDN access will replace the MCDN, as NCR ComTen equipment used on MCDN has the gateway capability for DDN.

C. AREAS FOR FURTHER STUDY

1. Cost-Benefit Analysis

A cost-benefit analysis is needed to compare the message costs at the DMS Baseline phase with DMS Phase I costs. DMS has a revolutionary impact on procedures for existing message systems and potentially has a similar impact on the costs associated with sending messages. The quantitative analysis to demonstrate and validate the increase in effectiveness due to DMS is needed to continue the DMS transition process.

2. GOSIP Tactical Implications

The mandate to comply with GOSIP for all protocol applications after August 1990 has a potential impact on the interoperability of existing tactical communications systems. A study on this topic would reveal possible shortcomings and identify possible solutions for these shortfalls. GOSIP is intended to provide a protocol standard from which implementations are constructed, hopefully in compatible systems. Systems which were built prior to GOSIP standardization efforts may not be compatible with succeeding systems.

3. Communications and Computer Functionality Merger

The convergence of computers and communications functionalities is accentuated in DMS and offers an opportunity to consolidate resources. Communicators have a greater need to understand computer operations and technology. Data processing personnel have a greater need than before to understand communications technology and organizational needlines. These two disciplines have such a great deal of functional overlap that there may be no need to distinguish between them. The training pipeline and general user orientation may require the merger of the two within a single occupational specialty.

4. Computer Viruses

Cryptographic devices do a superb job of shielding the network from intrusions, but do not safeguard against insidious attacks such as computer viruses, etc. The constantly changing virus strains poses a significant threat and highlights a need for a universal virus detector. A study on this topic could develop anti-viral procedures and increase awareness of how to counteract this threat.

D. CLOSING REMARKS

The transition to DMS within DOD has a significant impact on the way that the Marine Corps transmits messages. Tremendous processing power and effectiveness is placed within an organization's computer resources in this concept. The migration to DMS and OSI standards offers a unique opportunity for the Marine Corps to tailor information systems resources to meet organizational needs. This customization promises much flexibility, similar to the Marine Corps flexibility as an air-ground team.

APPENDIX A. ACRONYMS

Acronym	*Definition*
ACC	Access Control Center
ACP	Allied Communication Publication
ADI	AUTODIN-to-DDN Interface
ADP	Automated Data Processing
ADR	Address
AFAMPE	Air Force Automated Message Processing Equipment
AGT	AUTODIN Gateway Terminal
AIS	Automated Information System
AMME	Automated Multi-Media Exchange
AMPE	Automated Message Processing Equipment
ARPANET	Advanced Research Project Agency Network
ASC	Automated Switching Center
ASD(C^3I)	Assistant Secretary of Defense Command, Control, Communications, and Intelligence
AUTODIN	Automatic Digital Network
BER	Bit Error Rate
BFE	BLACKER Front End Device
BITS	Base Information Transfer System
BIU	Bus Interface Unit
CCITT	International Telephone and Telegraph Consultative Committee
COS	Corporations for Open Systems
COTS	Commercial Off the Shelf
CSP	Communications Support Processor
DAB	Defense Acquisition Board
DCS	Defense Communication Agency
DD-1392	Automated AUTODIN message release form
DD-173	AUTODIN Optical Character Reader message form
DDN	Defense Data Network
DECNET	Digital Electronics Corporation Network

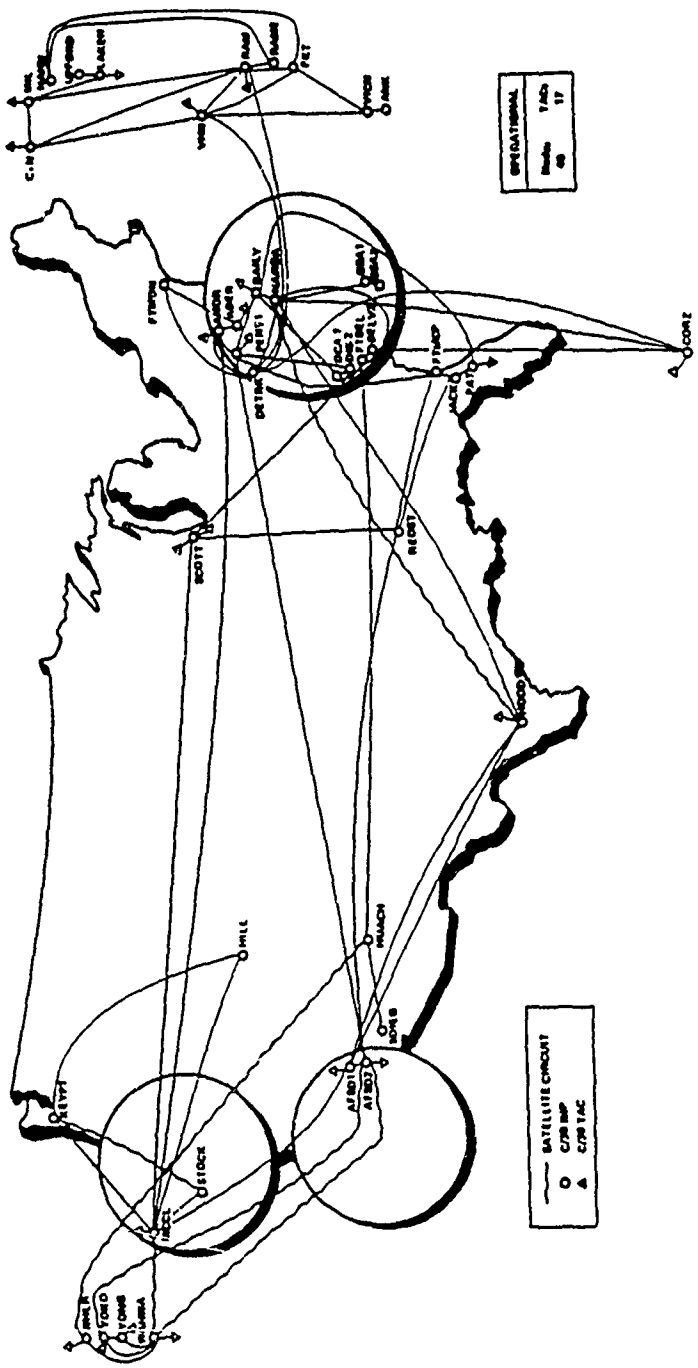
DIR	Directory
DISNET	Defense Integrated Secure Network
DSA	Directory System Agent
DSN	Defense Switching Network
DSNET	Defense Secure Network
DUA	Directory User Agent
E-Mail	Electronic Mail
E^2	End-to-End encryption
FEP	Front End Processor
FIPS	Federal Information Processing Standard
FMF	Fleet Marine Force
FTAM	File Transfer, Access, and Management
FTP	File Transfer Protocol
GC	Global Component
GOSIP	Government Open Systems Interconnection Profile
HDLC	High-level Data Link Control
IC	Installation Component
IDCS	Integrated Defense Communications System
IITS	Installation Information Transfer System
INTERNET	Internetwork (DDN)
ISDN	Integrated Services Data Network
ISM	Information Systems Management
ISO	International Standards Organization
ISODE	International Standards Organization Development Environment
JCS	Joint Chiefs of Staff
KDC	Key Distribution Center
LAN	Local Area Network
LDMX	Local Digital Message Exchange
MAD	Message Address Directory
MAN	Metropolitan Area Network
MCB	Marine Corps Base
MCDN	Marine Corps Data Network

MCEB	Military Communications-Electronics Board
MDS	Message Dissemination System
MGMT	Management
MHS	Message Handling System
MILNET	Military Network
MLS	Multi-Level Secure
MOTIS	Message Oriented Text Interchange System
MSA	Message Storage Agent
MTA	Message Transfer Agent
MTCC	Marine Telecommunications Center
MTF	Message Text Format
MTS	Message Transfer System
MTT	Message Teller Terminal
NAC	Network Access Component
NARDAC	Naval Regional Data Automation Center
NAVCOMMSTA	Naval Communication Station
NAVCOMPARS	Naval Communications Processing and Routing System
NDCCA	Naval Data Communications Control Architecture
NDI	Non-Developmental Item
NFS	Network File Server
NIST	National Institute of Standards and Technology
NMC	Network Management Center
NOS	Network Operating System
NS	Network Server
NTP	Naval Telecommunications Publication
OC	Organizational Component
OCRE	Optical Character Reader Equipment
OSI	Open Systems Interconnections
OSU	Optical Scanning Unit
OTC	Over-the-Counter
OUA	Organizational User Agent
PC	Personal Computer

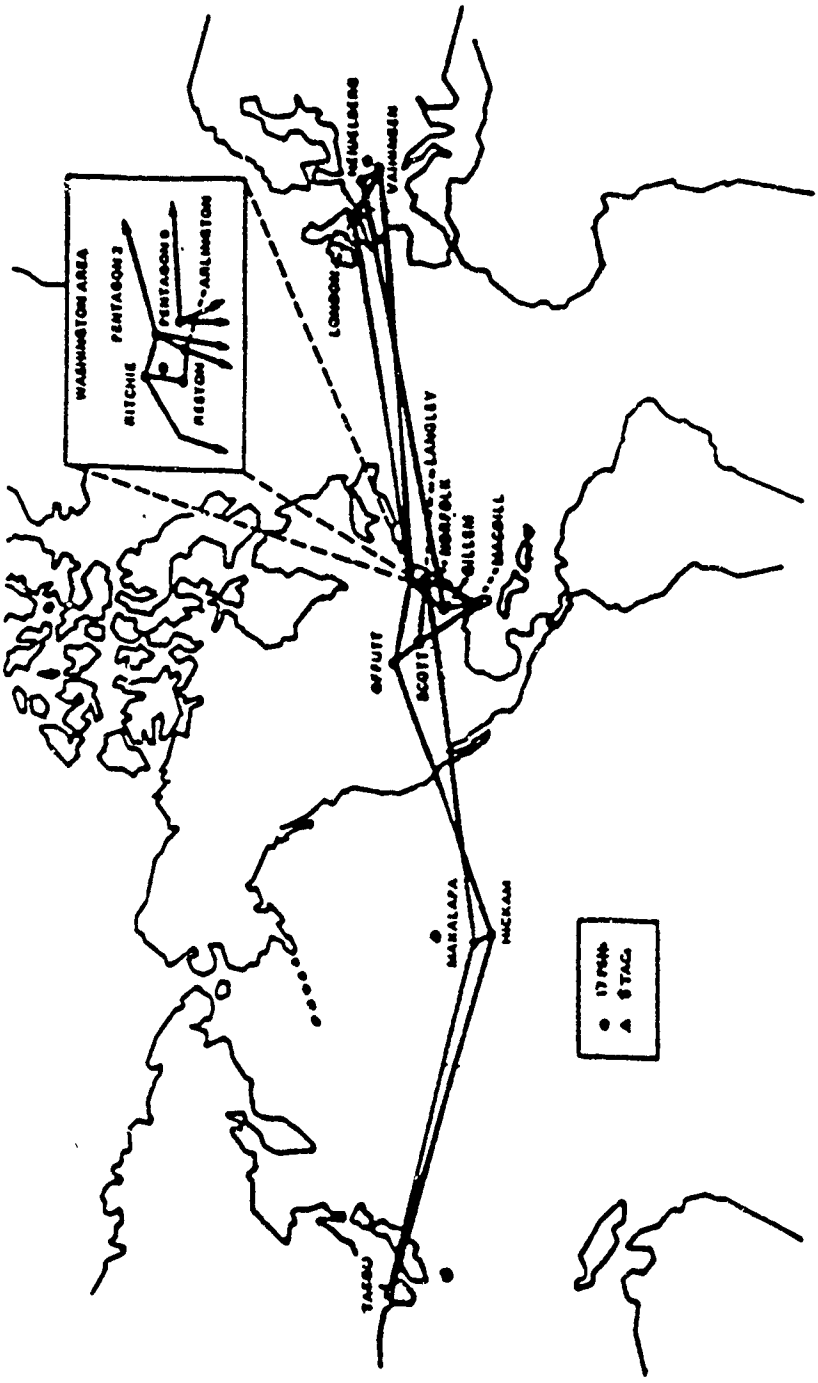
PCMT	Personal Computer Message Terminal
PLA	Plain Language Address
POSIX	UNIX-like Portable Operating System
RC	Regional Component
RI	Routing Indicator
RIXT	Remote Information Exchange Terminal
S/A	Service/Agency
SAC	Secure Access Card
SDLC	Synchronous Data Link Control
SDNS	Secure Data Network System
SE	Supporting Establishment
SMTP	Simple Mail Transfer Protocol
SNA	System Network Architecture
SSIC	Standard Subject Indicator Code
STU-III	Secure Telephone Unit Model III
TAC	Terminal Access Controller
TAIS	Target Architecture Implementation Schedule
TCC	Telecommunications Center
TCP/IP	Transmission Control Protocol/Internetwork Protocol
TEP	Terminal Emulation Processor
TERM	Terminal
TGG	Trusted Guard Gateway
TOUA	Trusted Organizational User Agent
TR	Transition Approach
T1	1.544 Mbps multiplexing carrier
UA	User Agent
UC	User Component
USJMTF	United States Joint Message Text Format
VINES	Virtual Network System
WORM	Write Once Read Many
WP	Word Processor
WWMCCS	Worldwide Military Command and Control System

APPENDIX B. DDN NETWORK STRUCTURE

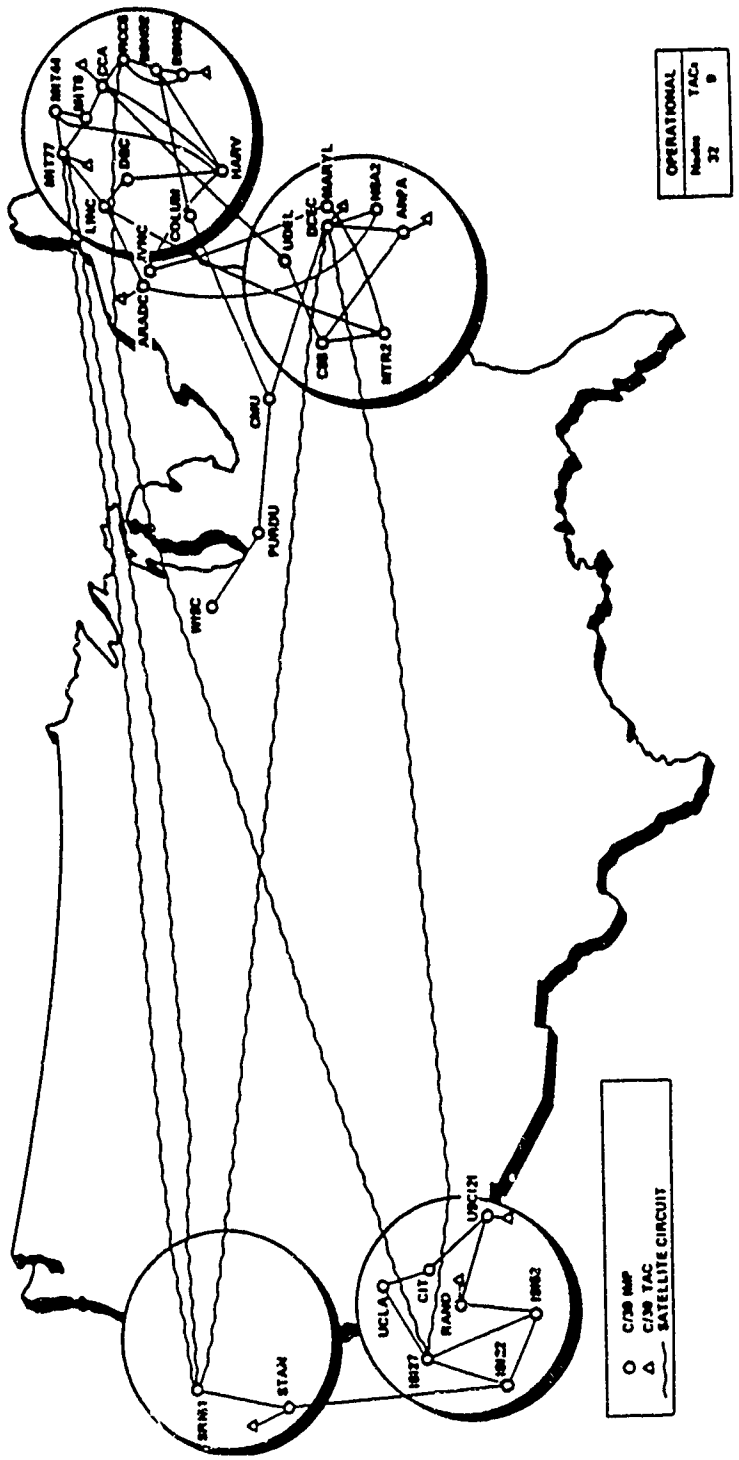
DISNET Network Structure



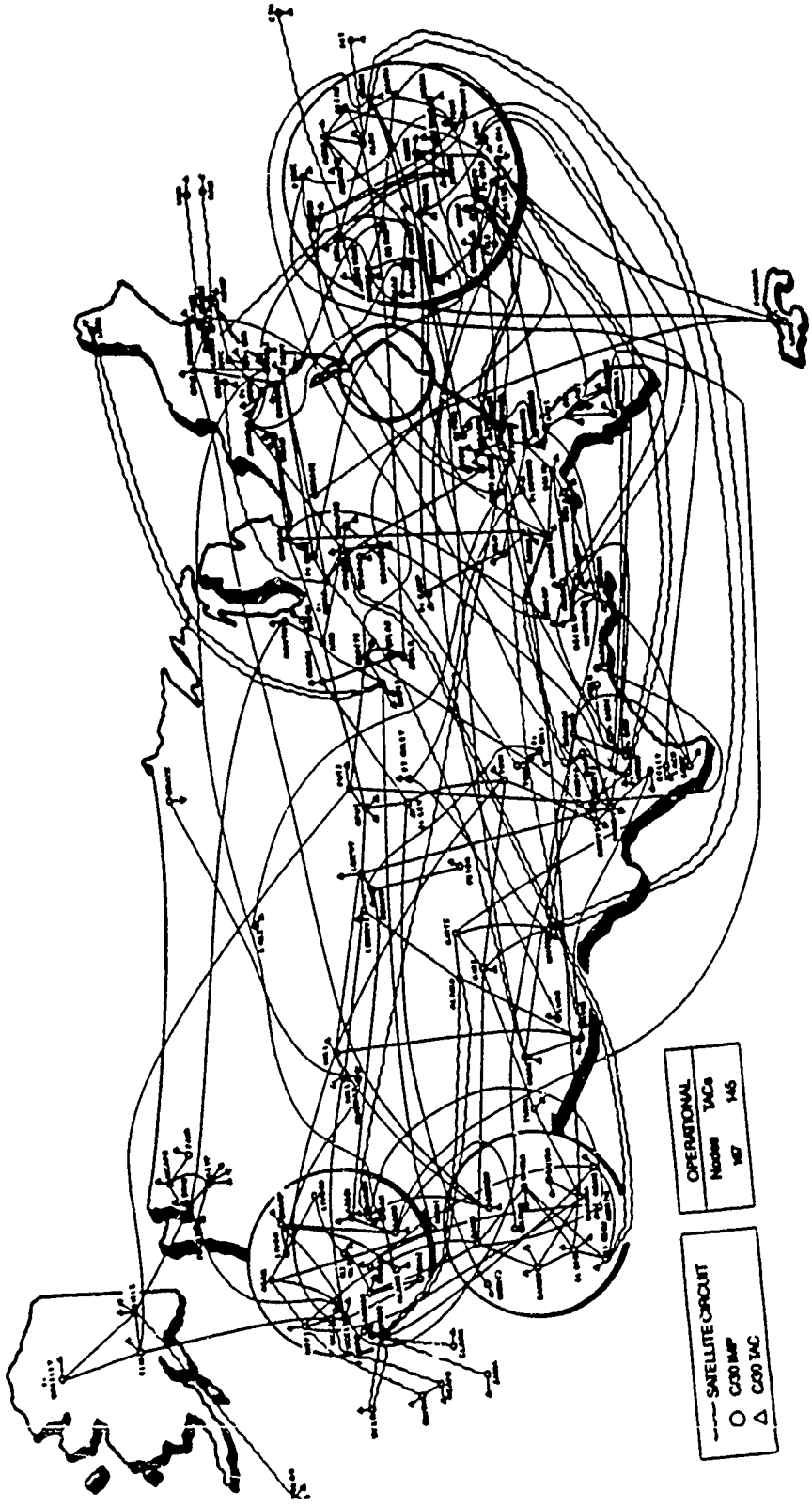
WWMCCS Information Network Structure



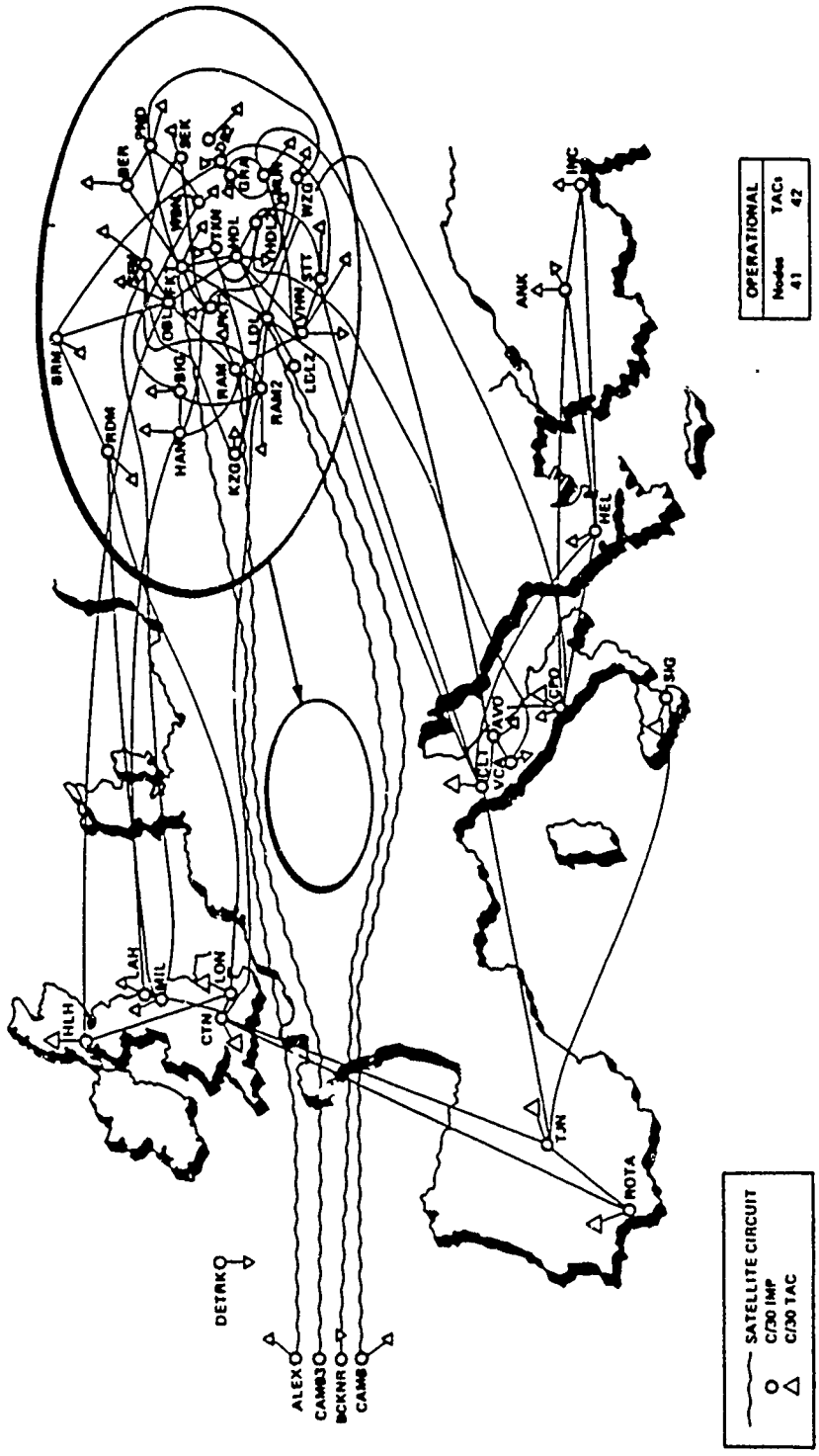
ARPANET Network Structure



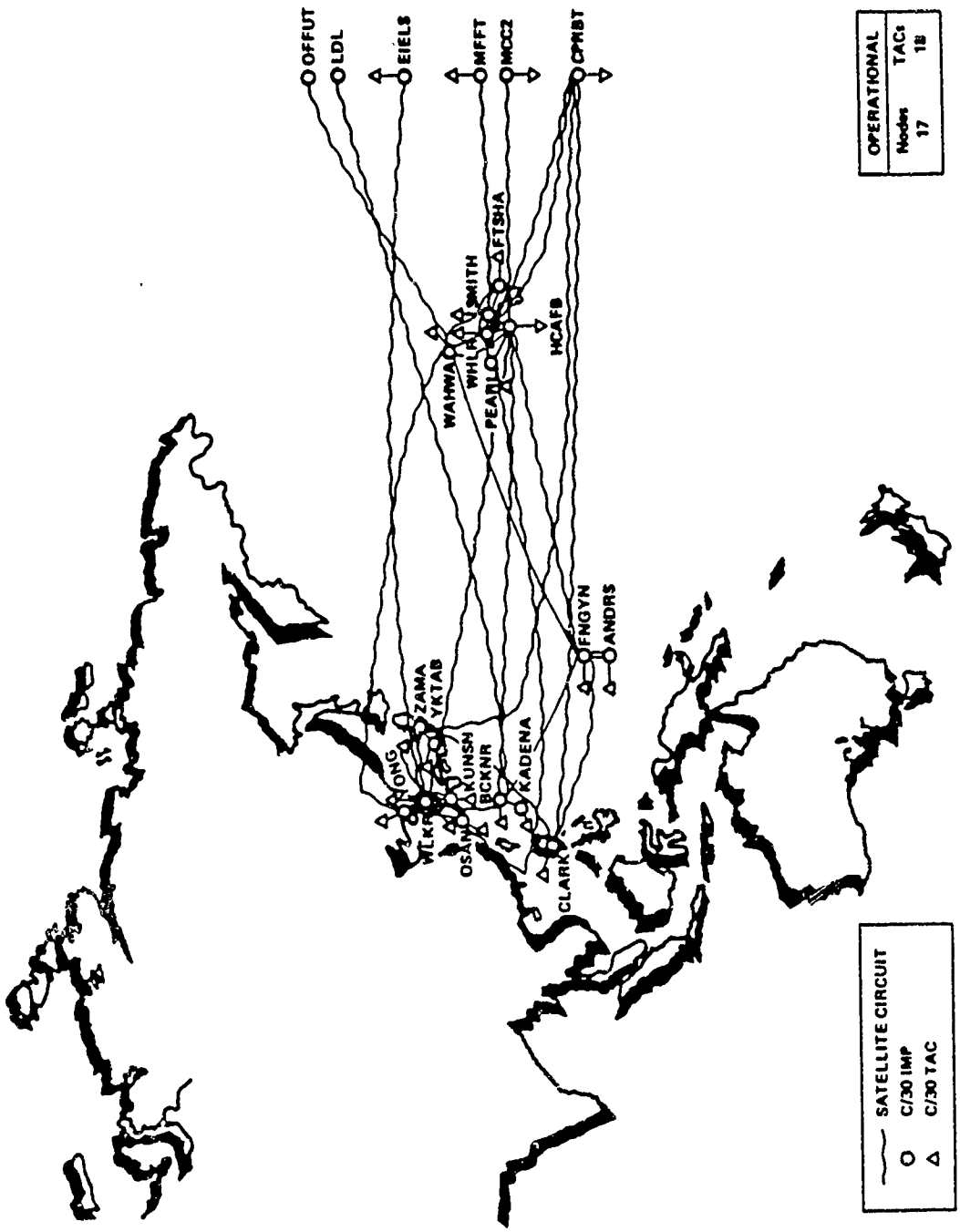
MILNET-U.S. Network Structure



MILNET-Europe Network Structure



MILNET-Pacific Network Structure



APPENDIX C. JANAP-128 MESSAGE FORMAT FIELDS

PARTS	COMPONENTS	FORMAT LINE	ELEMENTS	CONTENTS	EXPLANATION
HEADING	PROCEDURES	1	Handling instructions	Transmission identification for modes II, IV, and V stations only, and pilots	Contains start of message indicators and transmission identification when necessary (para. 403); contains pilots as required (para. 328 & 504).
		2	Header	Precedence, LMF, classification, CIC/CAI, OSRI, SSN, Date-Time filed, record count (as required), Classification(s) End-of-Routing signal.	If message is dual precedence, only the higher precedence is shown in this line.
		3	Calling station & filing time	Prosign DE: Routing Indicator of station preparing message for transmission; station serial number; filing time	Filing time is the date & time the message was filed with the communications center. Not used in AUTODIN originated message. Will be received in messages from other teletypewriter networks.

PARTS	COMPONENTS	FORMAT LINE	ELEMENTS	CONTENTS	EXPLANATION
HEADING	PROCEDURES	4	Transmission instructions	Security warning operating signal; classification designators; prosign T; other operating signals; special operating group(s) (SOGS); address designator(s); routing indicator(s)	Operating signals ZNR/ZNY, as appropriate and classification designators will be used. Indicates specific transmission responsibility not apparent in other components of the messge heading. Plain Language Designators are not permitted in CODRESS messages.
	PREAMBLE	5	Precedence; DTG; message instructions.	Precedence prosign, date, ZULU time, abbreviated month & year, operating signals.	In the case ofdual precedence, both prosigns are shown separated by a space. Operating signals are used only when required to convey message handling instructions.
	ADDRESS	6	Originator	Prosign FM; originator's designation	Message originator is indicated by plain language, RI, address group, or call sign.

PARTS	COMPONENTS	FORMAT LINE	ELEMENTS	CONTENTS	EXPLANATION
HEADING	ADDRESS	7	Action addressee(s)	Prosign TO; RIs; operating; signal; address designation(s).	Action addressee(s) is indicated by plain language, RIs, address group(s) or call sign(s). In the case of multiple address messages, when addressees are listed individually, each address designation shall be on a separate line & may be preceded either by the operating signal ZEN (meaning delivered by other means) or by the RI of the station responsible for delivery. Such use is mandatory on all joint & combined messages.
		8	Information addressee(s).	Prosign INFO; RIs; operating signal(s).	Same as for line 7, except that line 8 pertains to information addressee(s).

PARTS	COMPONENTS	FORMAT LINE	ELEMENTS	CONTENTS	EXPLANATION
HEADING	AD-DRESS	9	Exempt addresse(s)	Prosign XMT; Address designator(s).	Used only when a collective address designation is used in line 7 or 8 or an AIG indication of the addressee(s) exempted from the collective address or AIG is required.
	PREFIX	10	Accounting information; Group count, Program designator code.	Accounting symbol prosign ACCT, accounting symbol, group count prosign GR, group count dash (-) PDC.	The group count prosign & group count shall be used only when the text consists of countable encrypted group. PDC must be preceded by a dash (-) following the accounting symbol or group count.
	SEPARATION	11		Prosign BT	
		12A	Security classification, the abbreviation UNCLAS, or the word CLEAR.		See ACP 121 series. Classification and internal instructions not required in CODRESS or DATA PATTERN messages.
		12B	Special Handling Designations.	SPECAT; SIOP-ESI; US-UK EYES ONLY; etc.	If required, includes LIMDIS, EXDIS, & NODIS.

PARTS	COMPO-NENTS	FOR-MAT LINE	ELEMENTS	CONTENTS	EXPLANATION
HEADING	SEPA-RATION	12C	Releasability statements, or appropri-ate regional defense or-ganization security clas-sification statement.		If required, see para 355, ACP-121 US SUPP-1.
		12D	Subject Indi-cator Code (SIC), Standard Subject Indi-cator Code (SSIC),Delivery Distributrion Indicator (DDI).		If required, for SIC see para 323.d., ACP 121 US SUPP-1; SSIC (USN/USMC); DDI (NSA/CSS).
		12E	Special delibery in-structions, contents FOR, FROM, PASS TO ___, PER-SONAL FOR, etc.		If required.
		12F	Exercise Name.		If required.

PARTS	COMPONENTS	FORMAT LINE	ELEMENTS	CONTENTS	EXPLANATION
HEADING	SEPARATION	12G	Subject	SUBJ	See para 323.b. ACP 121 US SUPP-1. The letters "SUBJ" also serve as a delimiter in PLAINDRESS messages to identify the end of information pertaining to security and handling and that portion of textual information which must appear in every section of a sectionalized message.
	ADDRESS	12H	Reference(s)		If used.
		12I	Thought or idea		
		13		Prosign BT	
	PROCEDURE	14	Confirmation		Not used in AUTODIN and tape relay operations.

PARTS	COMPO-NENTS	FOR-MAT LINE	ELEMENTS	CONTENTS	EXPLANATION
ENDING	PROCE-DURE	15	Correction	Prosign C; other pro-signs; operat-ing signals & plain language as required.	Not used in DATA PATTERN mes-sages.
			EOM Vali-dation num-ber	Number sign (#) 4-digit number.	Used on all DOD orginated teletype-writer messages.
		16	EOM func-tions.	2CR, 8LF, 4Ns, 12LTRS.	Used on all tele-typewriter messages unless otherwise prescribed.
			or EOT	Repeats first 33 or 38 char-acters of header plus 4Ns.	Used only within AUTODIN.

APPENDIX D. MESSAGE TEXT FORMAT

SAMPLE RELEASING/RECEIPT DOCUMENT

Diskette Volume Label:

Originator's Unit/Organization:

Table-Of-Contents CRC Value:[1]

Classification of Diskette:

Signature of Releasing Officer:

L I S T O F M E S S A G E S[2]

FILENAME.EXT[3]	TYPE[4]	PRI[5]	CLASS	STATUS[6]	CRC[7]
121830.DEC	NA128	OO	UU	RECD	53169
121753.DEC	NA128	PP	SS	RECD	2248
111917.DEC	NA128	RR	CC	RECD	18975

---

1 TOC CRC value reflected is used to verify that the diskette has not been altered.

2 Software automatically prints message summary.

3 The filename assigned by user when preparing the message, or the name of the individual message file received by the NTCC. Users will not use DOS commands or "Diskette.TOC" as filenames. Use of these as filenames could cause some contents of the diskette to be altered or destroyed.

4 Message Type reflects the message format used, i.e. Native JANAP 128 (NA128), Narrative Message Prolog format (DD-173), etc.

5 Reflects the precedence and classification of the individual messages respectively.

6 This column will read REDY, for ready for form. When used as a Receipt Document, it will read RECD (Received Message).

7 CRC reflected for each message will be verified against the diskette TOC for each message when the TOC CRC values do not correspond. See paragraph 104 of NTP3G regarding discrepancies.

SAMPLE TABLE OF CONTENTS DISKETTE ENTRIES

TOC HEADER FORMAT

FORMAT_NAME	(M)
TABLE OF CONTENTS/V2	
TOC_CRC	(M)
:40193	
ORIGINATING_SYSTEM	(M)
: SARAV7-01	
CLASSIFICATION_OF_DISKETTE	(M)
: UU	
CREATION_DATE	(O)
:900329	
CREATION_TIME	(O)
: 07301578	
DISKETTE_RELEASING-OFFICIAL	(M)
: GEORGE OFFICIAL, COL	
ORGANIZATION	(M)
: TOP GUN SQUADRON, TNS/ME, 555-6677	
COMMENTS	(O)
MESSAGES_FOLLOW	(M)

---

8 (M) = Mandatory, (O) = Optional. These indicators are notpart of actual TOC header.

DD-173 PROLOGUE FIELDS WITH ALL OPTIONS[9]

FORMAT_NAME
: DD173
LMF
: AC
INTERNAL_MESSAGE_CRC
: 2478
COORDINATION_MEMO
: COORDINATION_REQUIRED
: MFR
FROM: CO
: These are the comments provided to correct
: or change this message. You can enter as
: many lines of input as needed to convey the
: information.
:
DISTRIBUTION
: EID/CC - 2
DRAFTERS_NAME
: SSGT I. M. FINE
DRAFTERS_OFFICE
: XPT/45410
RELEASERS_NAME
: BOSS/OIC/CSD42925
SPECIAL_INSTRUCTIONS
: CONFIRM DELIVERY TO ACTION ADDRESS
: TCC. SEND AS AS SINGLE ADDRESS
: MESSAGE
PAGE_OF
:01 01
DAY_TIME_ZULU
:290817Z

---

9 This is a prologue DD-173 message with a card output Language Media Format (LMF) using all mandatory and optional message information.

MONTH
: MAR
YEAR
:90
PRECEDENCE_FIRST
: PP
PRECEDENCE_SECOND
: RR
CLASS
: UU
SPECAT
:
CIC
: ZYVW
OMI
: XPP 031524 X
BOOK
: YES
MSG_HANDLING
: ZYQ
FROM
: CCSO TINKER AFB OK//SKAA//
TO
: HQ MAC SCOTT AFT IL//DO//I//
: COLLECTIVE NUMBER 21
INFO
: SSC GUNTER AFB GA//DO//I//
PLA_RI
: RUWTSUU
XMT
: HQ MAC SCOTT AFB IL
ACCT
: ARX GMRC
FL12A
: UNCLAS

FL12B
:
FL12B_COMMENT
: SVC ZUI SVC 0245 RUEDCSA1234 1921600.
FL12C
: INFORMATION ALLOWED BY PARA 355 ACP 121 US SUPP-1
FL12D
: SSIC CODE AND INFORMATION.
FL12E_H
: SPECIAL DELIVERY INSTRUCTIONS
: EXERCISE NAME
: SEE PARA. 323.b ACP 121-1
: REFERENCES
DECLASSIFICATION_INSTRUCTIONS
: DECLASSIFY AFTER 120 DAYS
TEXT_LINES_FOLLOW
THIS IS THE TEXT OF A MESSAGE AND NOTICE THAT
IT IS NOT REQUIRED TO BE PRECEDED BY A COLON.
(((END OF FILE MARK)))

DD-173 PROLOGUE EXAMPLE WITH NO OPTIONS[10]

```
FORMAT_NAME
: DD173
LMF
: AC
DAY_TIME_ZULU
:291700Z
MONTH
: MAR
YEAR
:90
PRECEDENCE_FIRST
: PP
CLASS
: UU
SPECAT
:
FROM
: CCSO TINKER AFB OK//SKAA//
TO
: HQ MAC SCOTT AFB IL//DO/LG//
: COLLECTIVE NUMBER 21
FL12A
: UNCLAS
TEXT_LINES_FOLLOW
THIS IS THE TEXT OF A MESSAGE AND NOTICE THAT
IT IS NOT REQUIRED TO BE PRECEDED BY A COLON.
(((END OF FILE MARK)))
```

---

10 A prologued DD-173 card output Language Media Format (LMF) using only mandatory message information.

JANAP 128 NARRATIVE MESSAGE WITH ALL OPTIONS[11]

FORMAT_NAME
: NR128
LMF
: CA
C_MESSAGE
: N
INTERNAL_MESSAGE_CRC
:90553
COORDINATION_MEMO
: COORDINATION COMPLETE
· MFR
: FROM: CO
: These are the comments provided to correct
: or change this message. You can enter as
: many lines of input as needed to convey
: the information.
:
DRAFTERS_NAME
: SSGT I.M. FINE
DAY_TIME_ZULU
:291700Z
MONTH
: MAR
YEAR
:90
PRECEDENCE_FIRST
: PP
PRECEDENCE_SECOND
: RR
CLASS
: UU

---

11 A prologued JANAP-128 message with a narrative output Language Media Format (LMF) using normal (PLAINDRESS) format and using all mandatory and optional message information

SPECAT
:
CIC
: ZYUW
OSRI_PLA
: RUWTAAA/CCSC TINKER AFB OK
: / CONTINUATION LINE STARTS HERE
TO
: RUWTXZZ/HQ MAC SCOTT AFB IL//DO/LG//
: / CONTINUATION LINE STARTS HERE
: /COLLECTIVE NUMBER 22 (FOR J128 AND DD1392)
: RUWTABC/
: RUWTABB/
: RUWTACC/UNIT NAME PLA
INFO
: RUWDXAB/NOC COMM GRP USA
XMT
: UNIT NAME PLA
ACCT
: ARK GMRC
TRC
: BB
FL4_TEXT
: ZFD RUWTABC
: ZOV RUCLGBA2144 REROUTE OF RUEKJCS1234 0011530
FL12A
: UNCLAS
FL12B
:
FL12B_COMMENT
: SVC ZUI SVC 0245 RUEDCSA1234 1921600.
FL12C
: INFORMATION ALLOWED BY PARA 355 ACP 121 US SUPP-1
FL12D
: SSIC CODE AND INFORMATION.

FL12E_H
: SPECIAL DELIVERY INSTRUCTIONS
: EXERCISE NAME
: SEE PARA. 323.b ACP 121-1
: REFERENCES
TIME_OF_FILE
:0761315
ORIGINAL_STATION_SERIAL_NUMBER
:0233
DECLASSIFICATION_INSTRUCTIONS
: DECLASSIFY AFTER 120 DAYS
TEXT_LINES_FOLLOW
THIS IS THE TEXT OF A MESSAGE AND NOTICE THAT
IT IS NOT REQUIRED TO BE PRECEDED BY A COLON.
(((END OF FILE MARK)))

DD-1392 WITH ROUTING INDICATORS AND NO OPTIONS[12]

FORMAT_NAME
: P1392
LMF
: CA
C_MESSAGE
: S
PRECEDENCE_ACTION
: PP
CLASS
: UU
SPECAT
:
CIC
: ZYVW
OSRI_PLA
: RUWTAAA/CCSC TINKER AFB OK
TO
: RUWTAAA/CCSC TINKER AFB OK
: / CONTINUATION LINE STARTS HERE
: / COLLECTIVE NUMBER 22
: RUWTABC
: RUWTABB
: RUWTACC
FL12A
: UNCLAS
TEXT_LINES_FOLLOW
THIS IS THE TEXT OF A MESSAGE AND NOTICE THAT
IT IS NOT REQUIRED TO BE PRECEDED BY A COLON.
DECLASSIFICATION INSTRUCTIONS IF REQUIRED
SHOULD BE HERE IN TEXT.
(((END OF FILE MARK)))

---

12 A prologued with narrative output Language Media Format (LMF) using only mandatory message information.

LIST OF REFERENCES

1. J6 to the Joint Chiefs of Staff, *Pre-Draft Report by J6 to the Joint Chiefs of Staff on Required Operational Capability for the Defense Message System*, by LCol Landrum, 10 May 1988.

2. Defense Message System Implementation Group, *Defense Message System (DMS) Target Architecture and Implementation Strategy (TAIS)*, Command, Control, Communications and Intelligence (Information Systems), Washington, D.C., December 1988.

3. Defense Communications Agency, *AUTODIN Procedures*, JANAP-128, Washington, D.C., 1988.

4. Commander, Naval Telecommunications Command, *Telecommunications Users Manual*, NTP-3G, 1986.

5. Kille, S. E., *Mapping between X.400 and RFC-822 (RFC-897)*, University College, London, June 1986.

6. Under Secretary of Defense, Unclassified, Memorandum for the Military Departments, Directors, Defense Agencies, Directors, Joint Staff, OJCS, Subject: Defense Data Network (DDN) Implementation, 10 March 1983.

7. Network Strategies, Inc., Contract DCA-100-83-C-0062, *The DDN Course*, De Vere, Rosemary, and others, April 1986.

8. Deepinder, P. Sidhu, "Protocol Design Rules," *Protocol Design Specification, Testing, and Verification*, pp. 283-290, North-Holland Publishing Company, 1982.

9. Assistant Secretary of Defense, Command, Control, Communications, and Intelligence, Unclassified Memorandum for Secretaries of Military Departments, Chair-

man, Joint Chiefs of Staff, Directors, Joint Staff, Directors, Defense Agencies, Subject: Open Systems Interconnection Protocols, 2 July 1987.

10. Naval Data Automation Command, *Navy Base Information Transfer System (BITS) Sub-Architecture*, 7 July 1989.

11. Rose, Marshall T., *The Open Book, a Practical Perspective on OSI*, Prentice-Hall, Inc., 1990.

12. Cerf, Vinton G., Cain, Edward, *The DOD Internet Architecture Model, Tutorial: Computer Communicati.ns: Architectures, Protocols and Standards*, Computer Science Press, 1985.

13. Wood, David C., "Local Area Network Standards," *Data Communications, Networks, and Systems*, Howard W. Sams & Co., 1985.

14. Miller, Mark A., "Troubleshooting Local Area Networks using the OSI Model," *Microsystems Journal*, Vol 4, No 10, October 1988.

15. Jackson, Kelly, "Tailoring Networks for OSI," *Communications Week*, No 284, January 22, 1990.

16. DCA/DCEC (Code R130) Interoperability and Standards, *The Department of Defense Open Systems Interconnection (OSI) Implementation Strategy*, May 1988.

17. Green Jr., Paul E., "Protocol Conversion," *Network Interconnection and Protocol Conversion*, IEEE Press, 1988.

18. Green, Bob, "Case Studies in OSI Initiatives -- US Navy Initiatives,"paper presented at the Interop 89 Symposium, 3 October, 1989.

19. Tanenbaum, Andrew S., *Computer Networks*, 2nd Ed, Prentice-Hall, Inc., 1988.

20. Henshall, John, Shaw, Sandy, *OSI Explained, End-to-End Computer Communication Standards*, Ellis Norwood Limited, 1988.

21. Stallings, William, *Data and Computer Communications*, Macmillan Publishing Company, 1988.

22. Naval Telecommunications Automation Support Center, *Defense Message System (DMS) Transition Strategy*, Working Draft, 8 January 1990.

23. Rose, Marshall T., *The Open Book, a Practical Perspective on OSI*, Prentice-Hall, Inc., 1990.

24. Stallings, William, "A Network Security Primer," *Computerworld*, Vol XXIV, No 5, January 29, 1990.

25. Sparta, Inc., Contract No. DCA 100-87-C-0095, *TrustedGuard Gateway (TGG) Technology Assessment*, Solo, D., and others, February 2, 1989.

26. Kent, Stephen T., "Security in Computer Networks," *Protocols & Techniques for Data Communication Networks*, Prentice-Hall, 1981.

27. Price, Wyn L., "Encryption in Computer Networks and Message Systems," *Computer Message Systems*, North-Holland Publishing Co., 1981.

28. Marine Telecommunications Center, Camp Pendleton, California, *Message Automation Study Team (MAST) Report*, Barber, Wiley, and others, August 1989.

29. Commandant of the Marine Corps, Unclassified Letter CCIR-01, 5230 to Distribution List, Subject: Standardized Local Area Network (LAN), 17 April 1989.

30. Communication-Electronic Officer, Marine Corps Base Camp Pendleton, California, *Base Wide LAN*, 25 January 1990.

31. Chorofas, Dimitris N., *Designing and Implementing Local Area Networks*, McGraw-Hill Book Company, 1984.

32. The MITRE Corporation, *Navy Data Communication Security Architecture*, 9 November 1988.

33. Stallings, William, *Local Networks*, Macmillan Publishing Company, 1984.

34. Blackall, Vince, "Virtual Networks," *Systems International*,Vol 15, No 4, April 1987.

35. Wilkinson, Stephanie, "Novell to Provide NetWare Global Naming Services," *MIS Week*,Vol 11, No 5, January 29, 1990.

36. Bonwill, Brice, "Branching out with Banyan VINES," *PC Tech Journal*, Vol 7, No 3, March 1989.

37. Kirby, Grant, "Virtual Networking," *Business Software*, Vol 6, No 3, March 1988.

38. Sytek, Incorporated, Special Publication 500-96, *The Selection of Local Area Computer Networks*, 1982.

39. Wang, William, "Inside Banyan's VINES 3.0," *LAN Technology*, February 1989.

40. Naval Telecommunications Automation Support Center, *Defense Message System (DMS) Message Dissemination System*, Working Draft, 10 January 1990.

41. Naval Telecommunications Automation Support Center, *Message Teller Terminal (MTT)*, Concept Review, 2 November 1989.

42. Naval Telecommunications Automation Support Center, Document Number 15X0022A FD-01, *Defense Message System Gateguard Subsystem Functional Description*, 1 November 1989.

43. Stallings, William, "Interfacing to the Defense Data Network," *Signal*, Vol 42, No 12, August 1988.

BIBLIOGRAPHY

Ambler, E.,*Government Open Systems Interconnection Profile (GOSIP)*, U.S. Department of Commerce/National Bureau of Standards, April 1987.

Bartoli, Paul D.,*The Application and Presentation Layers of the Reference Model for Open Systems, Tutorial: Computer Communications: Architectures, Protocols, and Standards*, IEEE Computer Society Press, 1985.

Bernhard, Robert,"Breaching System Security," *IEEE Spectrum*, Vol 19, No 6, June 1982.

Buddenberg, R.A., *Ship-Shore Packet Switched Communications System*, Masters Thesis, Naval Postgraduate School, CA, June 1986.

Case, J., *A Simple Network Management Protocol (SNMP) (RFC-1089)*, University of Tennessee at Knoxville, April 1989.

Castueil, Didien S., Giovachino, Domenic L.,"The First All-in-one Local Network," *The Local Network Handbook*, McGraw-Hill Publications Comnpany, 1982.

Comer, D., *Internetworking with TCP/IP*, Prentice-Hall, 1988.

Crocker, D.H.,*Standard for the Format of ARPA Internet Text Messages (RFC-822)*, University of Delaware, August 1982.

Dahlmeier, M.C., *An Information Analysis and Software Design for a Personal Computer-Based Message Management System*, Masters Thesis, Naval Postgraduate School, CA, March 1987.

Davies, D.W., and others, *Computer Networks and their Protocols*, John Wiley & Sons, 1979.

Elliott, Ronald D.,"The Integrated Tactical Data Network," *Signal*, Vol 43, No 7, March 1989.

Ennis, Gregory B., Kaufman, David J., Biba Kenneth J.,*DOD Protocol Refere - Model*, Sytek, Inc., Sep 1982.

Estrin, Deborah, *Network Interconnection and Protocol Conversion*, IEEE Press, 1988.

Gee, K.C.E.,*Introduction to Local Area Computer Networks*, John Wiley & Sons, 1983.

Gien, Michel, Zimmerman, Hubert, "Design Principles for Network Interconnection." *Tutorial: Computer Communications: Architectures, Protocols, and Standards*, IEEE Computer Society Press, 1985.

Hammond, Joseph L., O'Reilly, Peter, J. P.,*Performance Analysis of Local Computer Networks*, Addis-Wesley Publishing Company, 1986.

Helmers, Scott A., *Data Communications, A Beginner's Guide to Concepts and Technology*, Prentice-Hall, Inc., 1989.

Helmreich, Reinhard,*Acceptance Research Strategies in Computer Message Systems*, Labor fuer Benutzerforschung Zen, 1985.

Kane, Tom, Morin, Don,"Fleet Marine Force End User Computing," *Signal*, Vol 43, No 8, April 1989.

Lee, A.M., *Electronic Message Transfer and Its Implications*, Lexington Books, 1983.

Madron, Thomas W.,*Local Area Networks, the Second Generation*, John Wiley & Sons, 1988.

Martin, J., *Telematic Society*, Prentice Hall, 1981.

Postel, J.,*Simple Mail Transfer Protocol (RFC-821)*,Information Sciences Institute, August 1982.

Walker, Stephen T.,*Computer and Communications Security*, Howard Sams & Co., 1985.

Weidert, M.T., *Integrated Services Digital Network (ISDN)*, Masters Thesis, Naval Postgraduate School, CA, June 1985.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria, VA 22304-6145	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, CA 93943-5002	2
3.	Chief of Naval Operations(OP-941) Navy Department Washington, DC 20350-2000	1
4.	Commandant of the Marine Corps Code TE06 Headquarters, U.S. Marine Corps Washington, D.C. 20380-0001	2
5.	Commander, Naval Telecommunications Command Naval Telecommunications Command Headquarters 4401 Massachussetts Avenue, N. W. Washington, DC 20394-5000	2
6.	Bill Bryson Naval Telecommunications Automation Support Center c/o NAVCOMMUNIT Washington Washington, DC 20397-5310	2
7.	Dan C. Boger Code AS/Bo Naval Postgraduate School Monterey, CA 93943-5002	2
8.	Headquarters Marine Corps Interoperability Division Attn: C2I-P4 The Pentagon, Room 3201 Washington, DC 20380	2
9.	Patrick Sullivan Defense Advanced Research Projects Agency DARPA.TTO 1400 Wilson Boulevard 10th Floor Arlington, VA 22209	1

10. Commanding General (BF3) — 3
Marine Corps Base
Camp Pendleton, CA 92055-5000

11. Cathy Smith — 1
The MITRE Corporation
1820 Dolly Madison Boulevard
McLean, VA 22102

12. Warren Loper — 1
Naval Ocean Systems Center
Code 412
San Diego, CA 92152

13. James Tontonoz — 1
Defense Communications Engineering Center
1860 Wiehle Avenue
Reston, VA 22090